NEC

InDECT

Quick Setup Guide
(InDECT 1.3.1)

NDA-32000
Issue 1.0

Contents of this manual are subject to change without prior notice at the discretion of NEC Enterprise Communication Technologies, Inc. This document has been prepared for the use of employees and customers of NEC Enterprise Communication Technologies, Inc. and may not be reproduced without prior written approval of NEC Enterprise Communication Technologies, Inc.

NEC, the NEC logo, and UNIVERGE are trademarks or registered trademarks of NEC Corporation.

Other products mentioned in this document are the property of their respective owners and are also subject to copyright, trademark, and intellectual property protection as applicable by law.

Copyright 2019

NEC Enterprise Communication Technologies, Inc.
3929 W. John Carpenter Freeway
Irving, TX 75063

InDECT – Software Licence Agreement

PLEASE READ THIS SOFTWARE LICENCE AGREEMENT ("LICENCE") CAREFULLY BEFORE USING THE INDECT SOFTWARE. BY USING THE INDECT SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENCE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENCE DO NOT USE THE SOFTWARE.

1. The Definitions

1.1. “Licence” means this Software Licence.

1.2. “Customer” means Software User.

1.3. “Software” means all InDECT Software, the subject of this Licence, including (a) the accompanying documentation and any Updates and (b) any Upgrades purchased by the Customer or provided by NEC at no cost pursuant to §5.2 below.

1.4. “Update” means minor Software release the primary purpose of which is to remove incompatibilities, apply corrections, enhance the stability or remedy technical faults in the Software.

1.5. “Upgrade” means major Software release the primary purpose of which is to add new functionality or enhance the performance of the Software.

2. The Licence

2.1. NEC grants the Customer a limited, non-exclusive, non-transferable, non-sub licensable Licence to use the Software, subject to the following conditions:

2.1.1. The Software may only be used on the System upon which it is first installed. Consent must be obtained beforehand if the Software is to be used on a different System.

2.1.2. The Software may not be copied except for internal back-up purposes.

2.1.3. The Software may not be modified, de-compiled, disassembled, reverse engineered, merged or de-coded in any manner whatsoever.

2.1.4. The Software shall be maintained in safe custody. Any unauthorised use, reproduction, distribution or publication of the Software must be prevented. If the Software comes into the possession of a third party NEC must be notified immediately.

2.1.5. This Licence is personal to the Customer. The Software or a copy thereof shall not be loaned, rented, leased, licensed, assigned or otherwise transferred. The Customer acknowledges NEC’s proprietary rights to the Software. No title or ownership to the Software is transferred. The Software shall not be used in any manner that would derogate from NEC’s proprietary rights in the Software. The Software is protected by applicable copyright laws and international treaty provisions.

2.1.6. The Software, including documentation relating thereto, contains confidential information. Such information shall not be disclosed to any third party, other employees or authorised agents of the Customer, without NEC's prior written consent.

2.1.7. The use of the Software shall be supervised and controlled in accordance with the terms of this Licence. The Customer shall ensure that its employees, subcontractors or agents who have authorised access to the Software are made aware of the terms of this Licence and comply therewith. The Customer shall maintain safe custody of the Software.

2.1.8. The Customer shall permit NEC during NEC normal business hours to audit use of the Software and verify its compliance with the above conditions.

3. Copyright

3.1. The Customer acknowledges that the Software and documentation are protected by European and International copyright laws. The Customer shall not, during or at any time after the expiry or termination of this Licence, permit any act that infringes that copyright. The Customer expressly agrees that it shall not copy the Software except for back-up purposes pursuant to §2.1.2, or distribute, modify, publicly display or publicly perform the Software.

3.2. Ownership: This is a Licence to use the Software. It is NOT an agreement for the sale of the Software. All worldwide ownership of and all rights, title and interest in and to Software, and all copies and portions thereof, including without limitation, all copyrights, patent rights, trademark rights, trade secret rights, inventions and other proprietary rights therein and thereto, are and shall remain exclusively in NEC and its licensors. The Customer's rights to use the Software are specified in this Licence, and NEC retains all rights not expressly granted to the Customer in this Licence.

4. Limited Warranty

4.1. Subject to §4.2 through 4.6, NEC warrants that for ninety (90) days from the purchase date of the Software, it will perform according to its specifications.

4.2. NEC shall repair or replace Software subject to a valid warranty claim made within the warranty period, either on-site or off-site, at NEC's discretion and during normal business hours. If the Customer asks NEC to provide services outside its normal business hours, it shall be charged for such services at NEC's standard after-hours rates. If it is not possible to repair or replace the Software, the Software licence fee shall be refunded. The remedies described in this §4.2 shall be NEC's sole obligation and the Customer's sole remedy in the event Software fails to perform according to its specifications during the warranty period. For support purposes, the Customer shall permit remote access to the Software, during normal business hours, upon request for support. The Customer recognises that NEC's ability to support the Software is dependent upon the Customer providing this remote access.

4.3. Because there is such a diverse range of telecommunications environments, NEC cannot warrant that the Software will be compatible in every operating environment. It is the Customer's responsibility to ascertain whether its own operating environment is compatible with the Software.

Any Software modifications which NEC may agree to make to achieve compatibility shall be at its prevailing rates and charges. NEC does not warrant that the Software will meet the Customer's requirements or that its operation will be uninterrupted or error-free. NEC does not warrant that the Software is free of errors or defects. The existence of such Software errors or defects shall not constitute a breach of this warranty. Notwithstanding the foregoing NEC shall provide the Customer with Software corrections for known errors that also affect NEC's other licensees. NEC excludes, and expressly disclaims, all express and implied warranties of merchantability or fitness for any particular purpose. NEC shall not be responsible for external factors affecting the performance of the Software, including without limitation, telecommunications and network breakdowns, power surges or interruptions and other "Acts of God".

4.4. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL NEC BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES ARISING OUT OF OR RELATED TO YOUR USE OR INSTABILITY TO USE THE NEC SOFTWARE, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF NEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

4.5. Some jurisdictions do not allow the exclusion of certain implied warranties or conditions, so the above exclusions may not apply to the Customer. This Licence does not exclude any implied warranties or conditions that may not under applicable law be excluded. In no event shall NEC total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of seventy five pounds (£75). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.

4.6. This Licence does not impose any obligations upon NEC to provide support and Software Assurance ("SA") services outside of the warranty period. Should the Customer require such services, they shall be obtained by arrangement with NEC Technical Services.

5. Other Services

5.1. If NEC provides services outside the coverage of its limited warranty or after it has expired, the Customer shall pay for such services at NEC's standard rates and charges, plus travel and accommodation if applicable.

5.2. To fix an error in the Customer's Software, it may be necessary to install an Upgrade containing both version enhancements and bug fixes. During the warranty period, NEC shall provide such Software Upgrade at no cost. After the warranty period, NEC shall provide such Upgrade at its standard price. In addition to the price of such Upgrade, the Customer shall pay us for any services that NEC provides pursuant to §5.1.

6. Termination/Cancellation

6.1. NEC may Terminate/Cancel this Licence if the Customer breaches any condition thereof. If the breach is capable of remedy, NEC shall give the Customer thirty (30) days written notice within which to do so. Otherwise, Termination/Cancellation shall take effect immediately upon the Customer's receipt of NEC's notice.

6.2. The Customer may Terminate/Cancel this Agreement upon forty five (45) days prior written notice to NEC. Upon the date of Termination/Cancellation, the Customer's Licence to use the Software shall be deemed revoked, the customer will no longer be bound by the terms of this Agreement. Payment for the Software remains unaffected by this clause; this clause does not grant any free period of usage.

7. Term of Licence

7.1. This Licence commences upon the Customer's acceptance hereof. It shall continue, in perpetuity, subject to termination by NEC in the event that the Customer breaches any term herein, or by the Customer with written notice as stipulated in §6.2.

7.2. Upon termination/cancellation the Customer or its representatives shall immediately stop using the Software and documentation and shall return, or destroy all copies of the Software and documentation in a manner directed by NEC.

8. Other Clauses

8.1. If NEC foregoes or delays enforcing an obligation or remedy under this Licence, such forbearance or delay shall not result in a waiver or variation of such obligation or remedy. No failure by NEC to insist upon strict performance of any term or condition in this Licence shall constitute a waiver or variation of such term or condition. Such failure shall not prevent NEC from claiming default or seeking a remedy under this Licence.

8.2. This is the entire agreement between NEC and the Customer. Upon agreeing to the terms of this Licence the Customer agrees that this Licence supersedes prior licensing agreements, both written and verbal for NEC Software.

8.3. This Agreement shall be governed by and construed in all aspects in accordance with the Laws of the jurisdiction in which NEC as the supplier of the Software is geographically based and each party submits to the non-exclusive jurisdiction of the courts in that geographic location.

8.4. The Customer acknowledges that a breach of this Agreement may cause irreparable and continuing damage to NEC for which money damages may be insufficient, and NEC shall be entitled to injunctive relief and/or a decree for specific performance and such other relief as may be proper (including money damages if appropriate). In the event of litigation between NEC and the Customer concerning Software or any other item which is subject to this Agreement, the prevailing party in the litigation will be entitled to recover legal fees and expenses from the other party.

8.5. If any part of this Agreement is found void and unenforceable, it will not affect the validity of the balance of the Agreement, which shall remain valid and enforceable according to its terms.

8.6. Acknowledgement. **BY INSTALLING SOFTWARE, THE CUSTOMER ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS.**

TABLE OF CONTENTS

Chapter 1 InDECT Quick Setup Guide

LIST OF FIGURES

Chapter 1 InDECT Quick Setup Guide

LIST OF TABLES

Chapter 1 InDECT Quick Setup Guide

Appendix A PBX Items Configured by InDECT

InDECT Quick Setup Guide

Chapter 1

SECTION 1 INTRODUCTION

InDECT is a toolset that can be integrated to either NEC's UNIVERGE SV9100 or SL2100 communication servers. It allows for easy installation, deployment and maintenance of a small scale IP DECT system with no additional IT servers required.

InDECT minimizes the installation effort by automatically retrieving settings such as regional, tone plan, SIP settings etc. from the PBX configuration, whilst enabling access points to download configuration files from the on-board file server with minimal intervention by the installation engineer to the end users network.

The user interface of InDECT consists of web pages that can be accessed by means of a web browser, so not requiring a dedicated PC configuration tool for installing or upgrading a system.

InDECT is part of the family of NEC's easy to use 'InApps' range of applications and future versions will include additional functionality as the application is developed further.

SECTION 2 LICENSING

License Code 3518 is required to run InDECT on the SV9100 or SL2100 communication servers, it can also run if the 60 day license is enabled.

The following LMS licenses are available for InDECT:

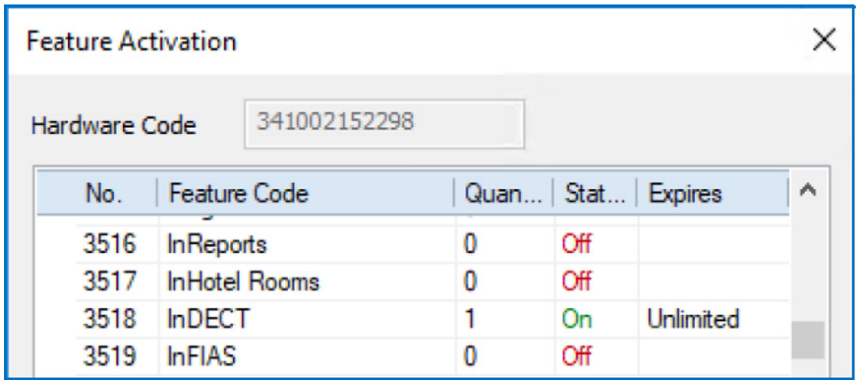
Table 1-1 LMS Licenses

PBX	Description
SV9100	SV9100 INDECT MANAGEMENT LIC
SL2100[1]	SL2100 INDECT MANAGEMENT LIC

[1] *The SDVMS or SDVML InMail memory cards can also be used. A 16GB MICROSDHC UHS-1 memory card can also be used, only if the system does not already have the SDVMS/L card added.*

When the license is installed, it can be viewed through PC Pro in **Feature > Activation** or **WebPro / TelPro**.

Figure 1-1 Feature Activation Screen



SECTION 3 REQUIREMENTS

It is NOT necessary for the PBX to be able to access the Internet. As with other InApps, the InDECT application can only be accessed using the http protocol. The supported platforms and minimum versions of system software required to run InDECT are as follows:

Table 1-2 PBX Version Requirements

PBX	System Software Version
SV9100	10.00 or above and CP20
SL2100	2.06 or above

NOTE

The SL2100 must have a memory card installed to run InDECT for storage of the application files. If an SDVMS or SDVML InMail memory card is installed, then this can be used. Otherwise, a 16GB MICROSDHC UHS-1 memory card can also be used when an InMail SD Card is not installed.

Table 1-3 InApp Manager Requirements

InApp Manager	Version
SL2100 & SV9100	1.7.0 or above

It is recommended that latest InApp Manager is installed prior to the installation of InDECT onto the PBX. The InApps and InApp Manager are available from the SL2100 & SV9100 Communication Platform areas.

SECTION 4 CAPACITIES

InDECT can support an IP DECT system up to a maximum capacity of 32 x AP400 access points. For systems up to 10 access points the AP400S can be used, while for larger systems (11-32 APs) the AP400C is required.

A maximum of 64 handsets can be used with an InDECT system. Supported devices include the following models:

G266/G277/G566/G577/G577h/I766

SECTION 5 TRAINING/DOCUMENTATION

InDECT is intended to be used by engineers with experience in the deployment of NEC IP DECT systems. Training videos for InDECT and IP DECT installation can be located at https://training.necam.com.

Available InDECT documentation includes:

- ❏ InDECT Quick Installation Guide (this document)
- ❏ InDECT Additional Information Manual
- ❏ Site Survey Manual IP DECT

SECTION 6 WEB BROWSERS

InDECT can be accessed using one of the following Web Browsers:

- ❏ Internet Explorer 11
- ❏ MS Edge
- ❏ Firefox
- ❏ Google Chrome

SECTION 7 NETWORK REQUIREMENTS

InDECT AP400 DAPs only require a basic DHCP server to provision them with a minimum IP configuration of an IP Address, Subnet Mask and optional Default Gateway. They will then automatically locate the PBX fileserver on the local network when running, and download the InDECT configuration files from here.

SECTION 8 INDECT INSTALLATION

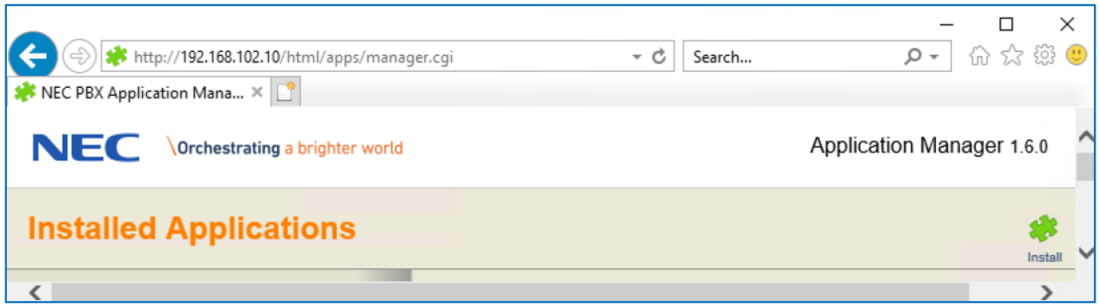
InDECT is installed using the application manager on the PBX, which can be accessed via the URL:

http://**IP Address of the PBX**/html/apps/manager.cgi

For example:
http://192.168.102.10/html/apps/manager.cgi

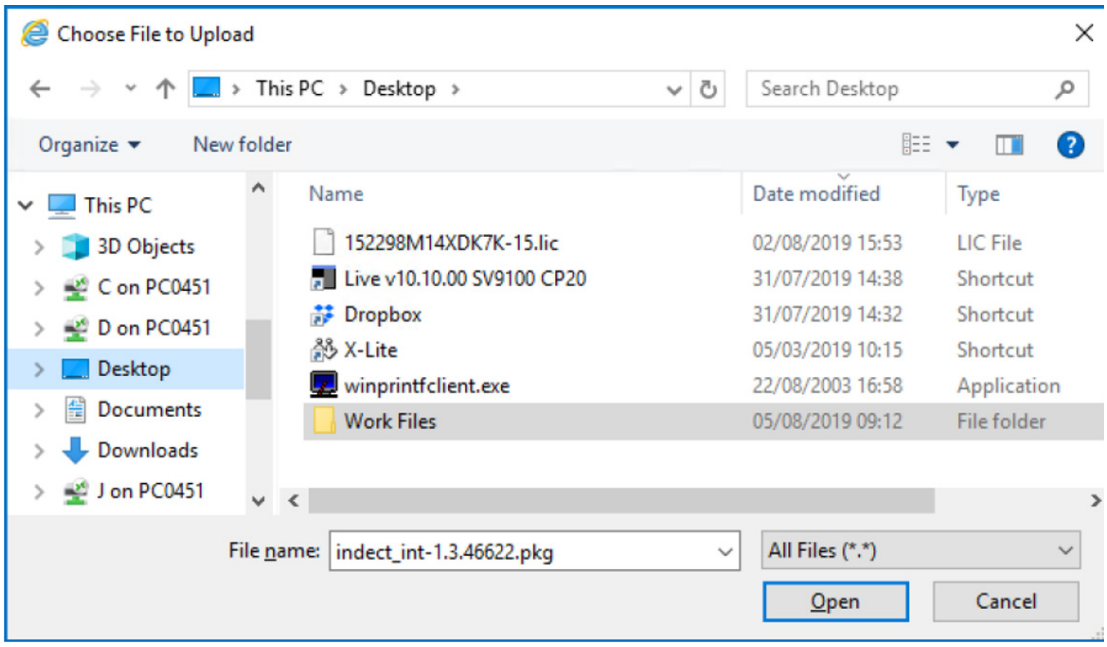
You will need to logon to the application manager with an installer account for the PBX. Once logged in, begin the installation process by pressing the **Install** button in the top right hand corner.

Figure 1-2 Application Manager Screen



1. Browse to the required InDECT pkg installation file and press **Open** to select it.

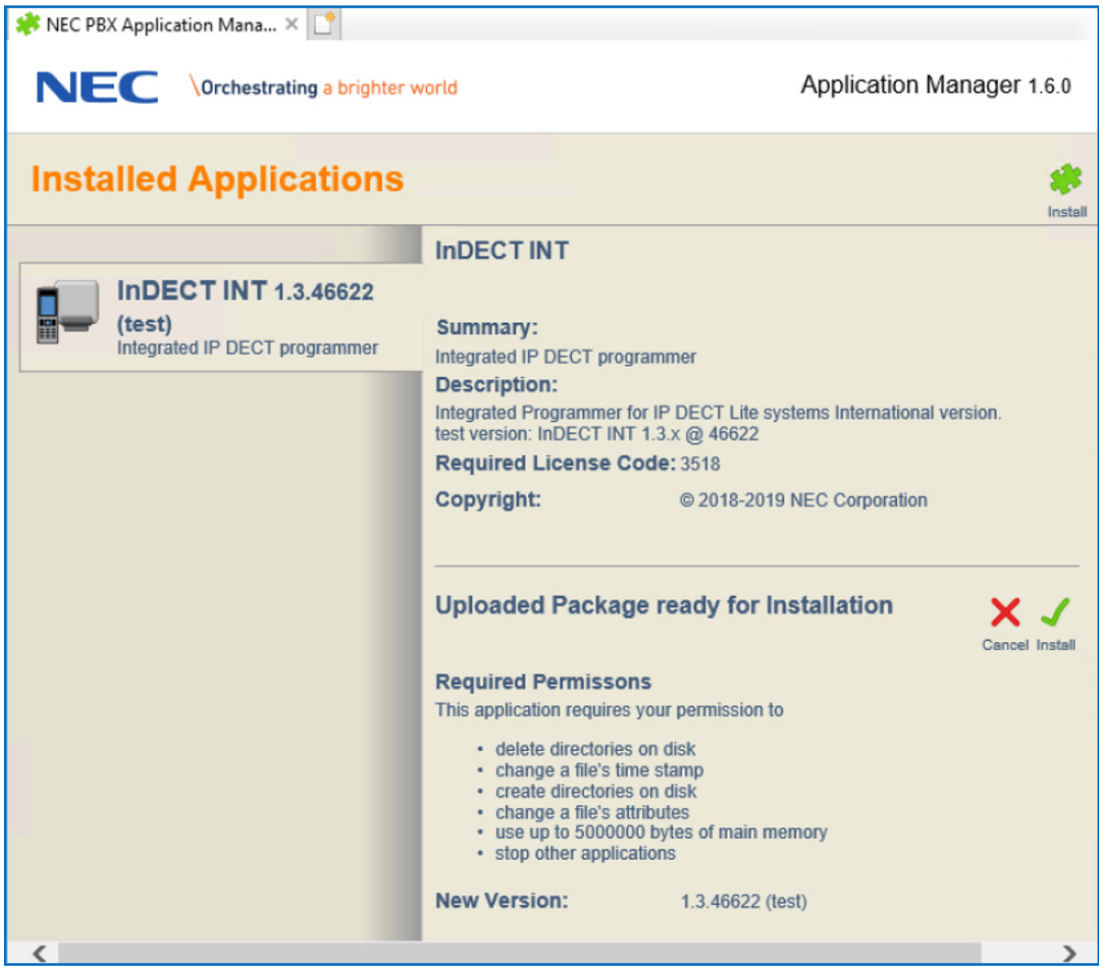
Figure 1-3 Choose File to Upload Screen



2. A preview of the application about to be installed is displayed in the lower half of the window. Press the green **Tick** 

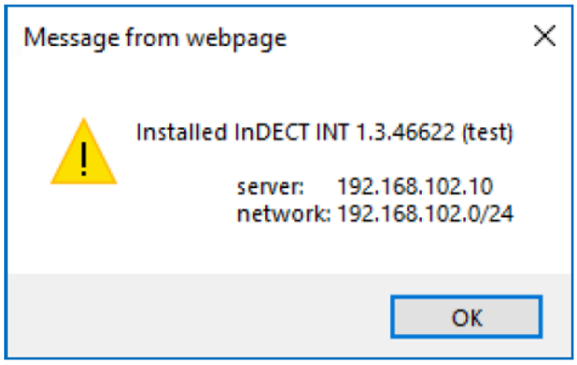
button to proceed with the install.

Figure 1-4 Software Installation Preview Screen



3. The installation process can take approximately 1 minute to complete. Once installed, a message window showing the network IP configuration of the PBX may appear.

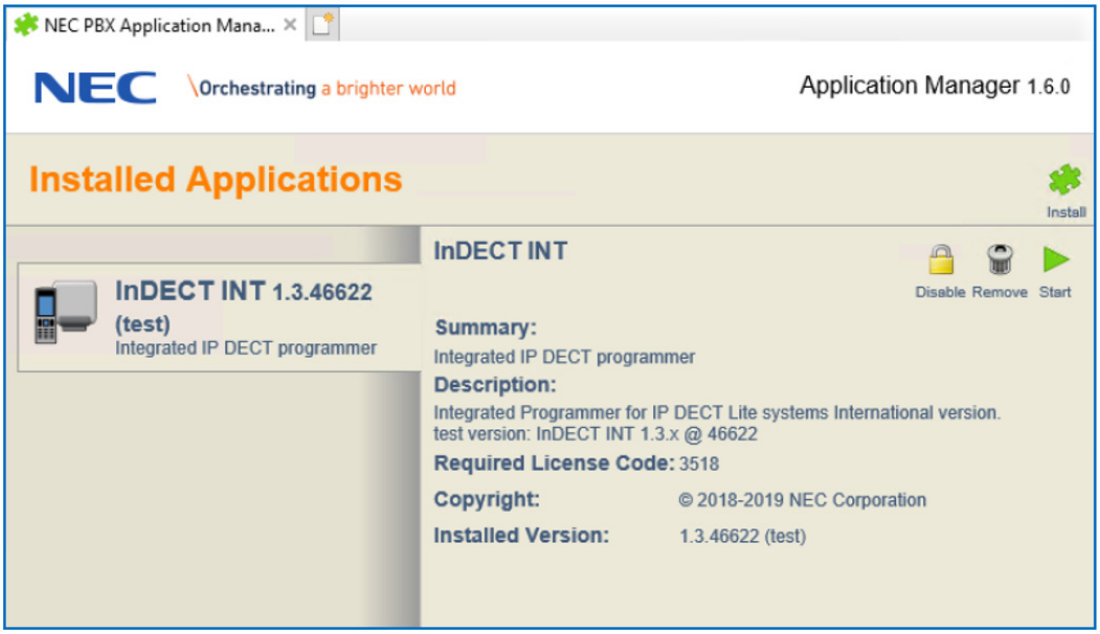
Figure 1-5 Software Installation Message



4. When the install successfully completes, press on the **Start** 

button. InDECT services start.

Figure 1-6 Start InDECT Services



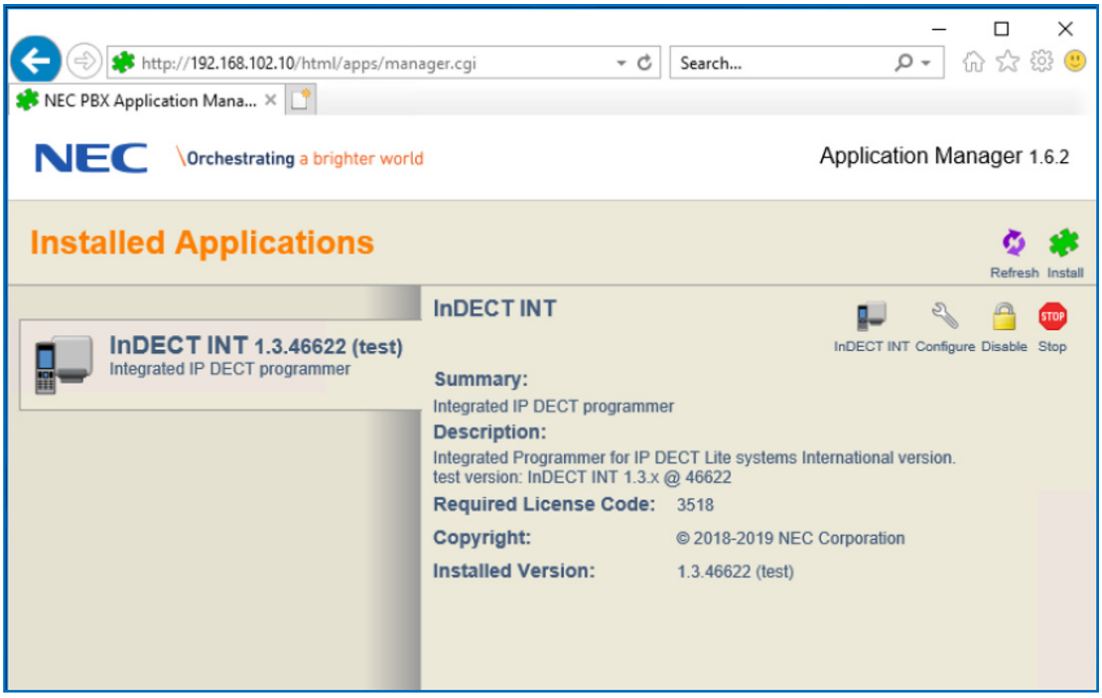
5. After InDECT is starts, you can press the red **Stop** 

button, at any time, to stop the application from running on the PBX.

6. The **Disable** 

button displays. If pressed, it will not stop the InDECT application, if it is currently running. However, it does prevent it from automatically starting, if the PBX is rebooted.

Figure 1-7 InDECT INT with Disable Button



7. If you wish to have the application run automatically when a reboot of the PBX occurs, press the **Enable** 

button.

InDECT is now installed and ready to be configured.

SECTION 9 LOGON TO INDECT

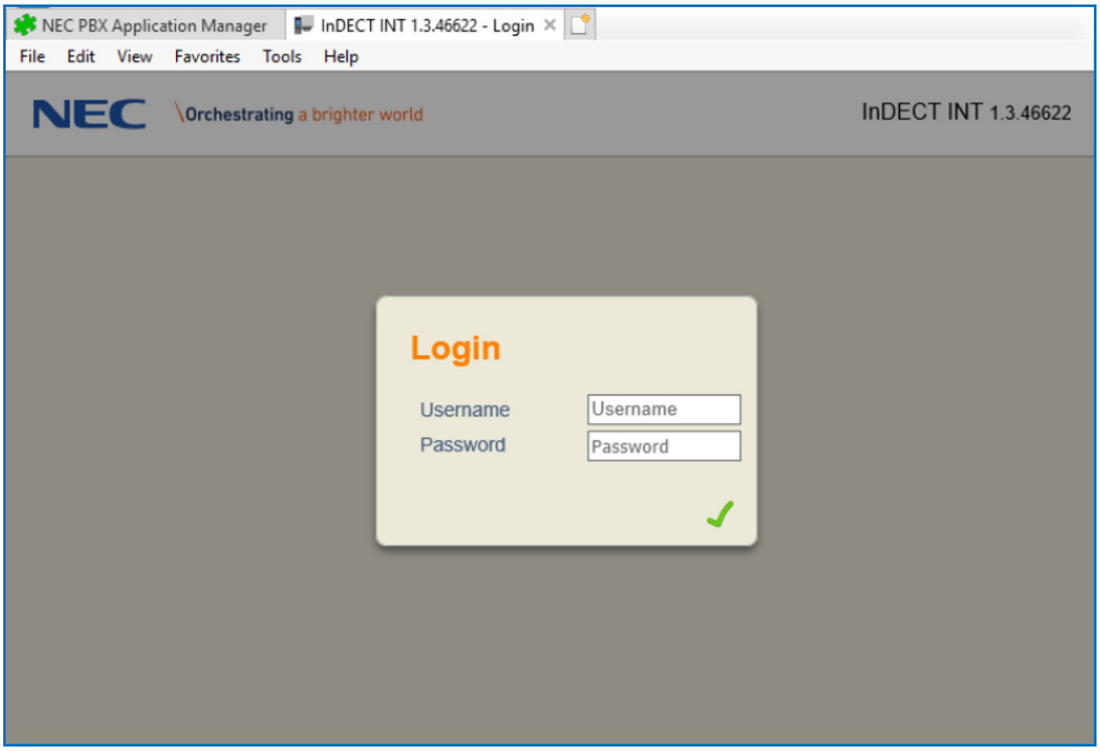
After InDECT is installed and started, you can press either the **InDECT INT** 

button or **Configure** 

button to open the InDECT interface.

The default username and password for logging on is tech / 12345678

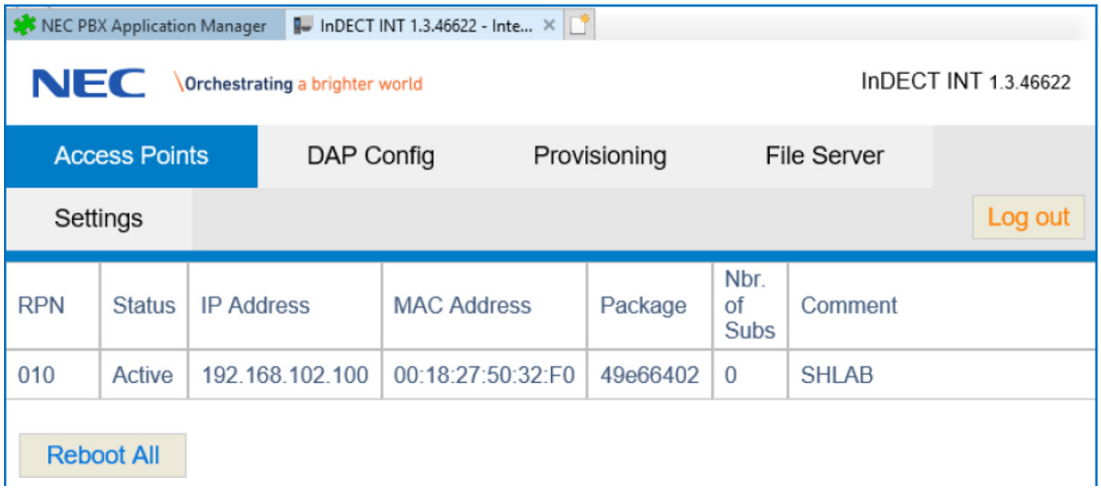
Figure 1-8 InDECT Login Screen



If you logon using the **InDECT INT** 

button, the **Access Points** screen displays. You have **read only** visibility of the InDECT configuration along with access to the **DAP Config**, **Provisioning** and **File Server** screens.

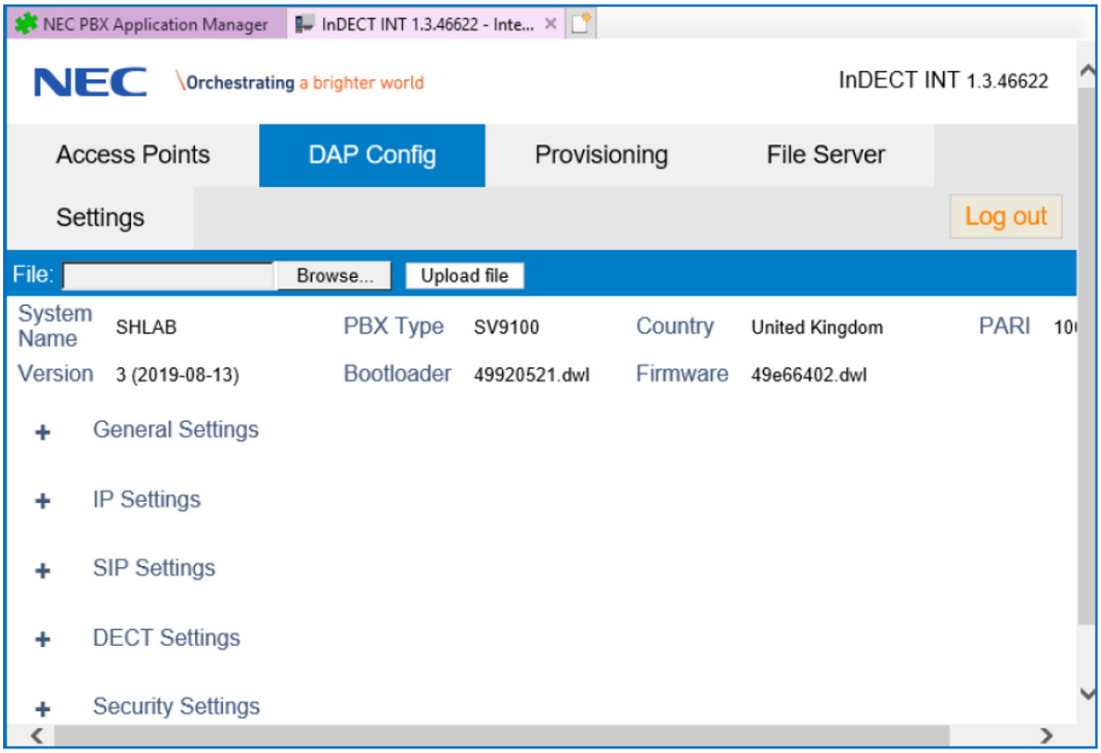
Figure 1-9 InDECT Access Points Screen



When you press the **Configure** 

button, the **DAP Config** screen displays. This scree is used to create a new system configuration or edit an existing system, if it is found on the PBX. This is where you normally start with a new installation.

Figure 1-10 InDECT DAP Config Screen

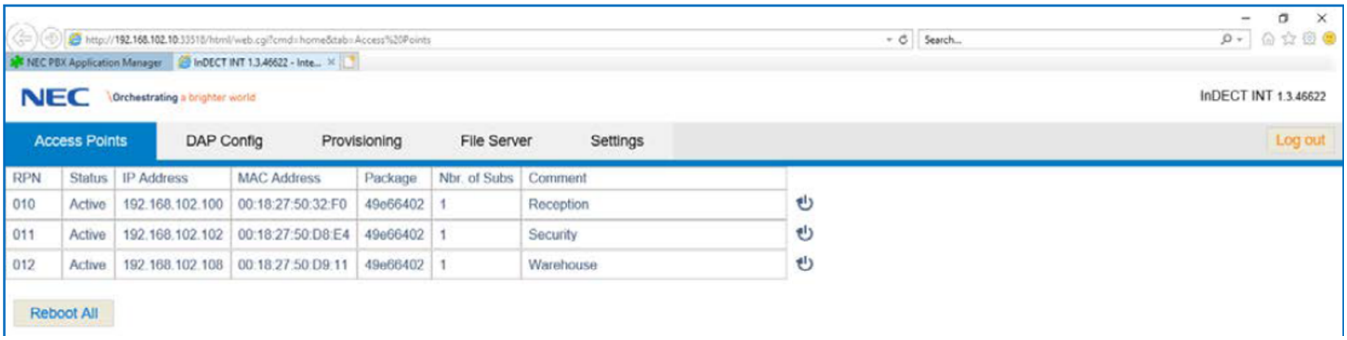


SECTION 10 OVERVIEW OF THE INDECT GUI

10.1 Access Point Screen

The **Access Points** screen lists details of DAPs detected by InDECT, located on the PBX network. You can see details about each DAP such as RPN number, allocated IP address from DHCP, MAC address, firmware package installed and the number of handset subscriptions.

Figure 1-11 InDECT Access Points – Reboot All



On the **Access Points** screen you can perform the following functions.

Table 1-4 Access Point Function Icons

Functions	Icon	Description
Reboot		Reboot an individual DAP.
Add DAP		Add a newly detected DAP on the network to the InDECT system configuration.
Remove DAP		Remove a non-operational DAP from the InDECT system.
Reboot All DAPS		Reboot all ‘Active’ DAPs connected to the InDECT system.
Edit RPN		You can double click any ‘Active’ DAPs RPN number to edit the existing value.
Edit Comment		You can double click any ‘Active’ DAPs Comment field to add a description of the DAP or location where it is placed.

DAP status descriptions are detailed in the below table.

Table 1-5 DAP Status Icons

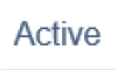
Functions	Icon	Description
New		InDECT has detected a DAP on the PBX network but it is currently not part of the system configuration or usable.
Active		An active DAP has been added to the InDECT system configuration and running normally.

Table 1-5 DAP Status Icons

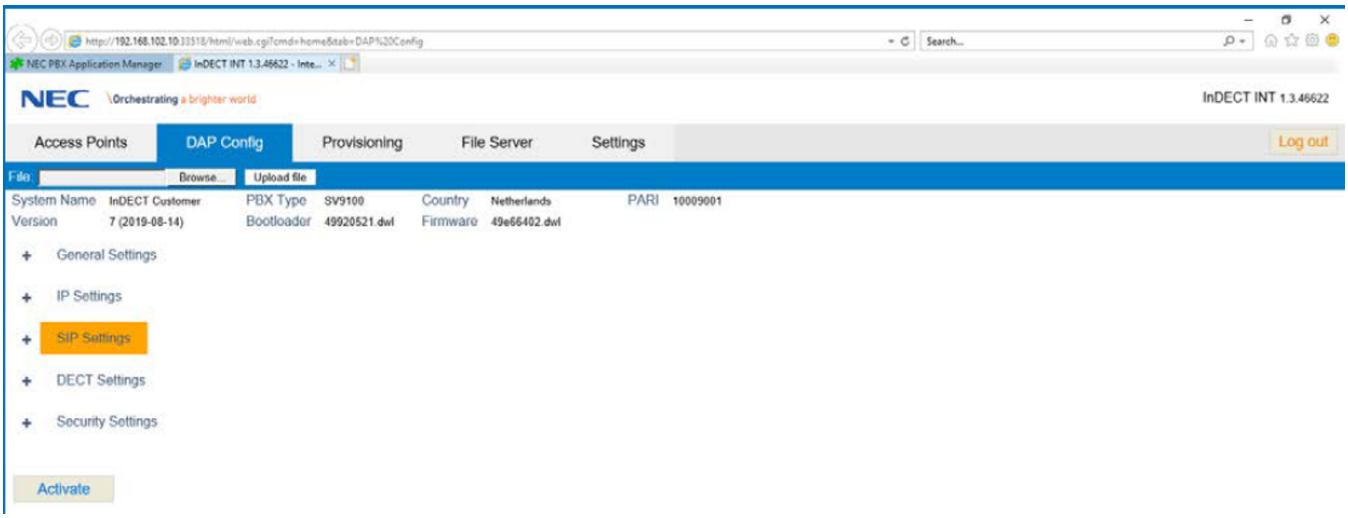
Inactive	Inactive	A DAP that was added to the InDECT system configuration is no longer contactable on the PBX network.

A DAP that is in an Inactive state can be deleted from the system by pressing the **Remove DAP** button that appears next to it.

10.2 DAP Config Screen

The **DAP Config** screen displays the InDECT system configuration. This is split into five sub areas; General Settings, IP Settings, SIP Setting, DECT Settings and Security Settings. At the top of the screen upload the DAP bootloader/firmware packages. Below that area are static details about the system, which include the system name, version number of the configuration file on the PBX fileserver, PBX type used, current bootloader/firmware used by the DAPs, the country selection used for tones/radio frequency settings and the InDECT PARI code.

Figure 1-12 InDECT DAP Config – SIP Settings



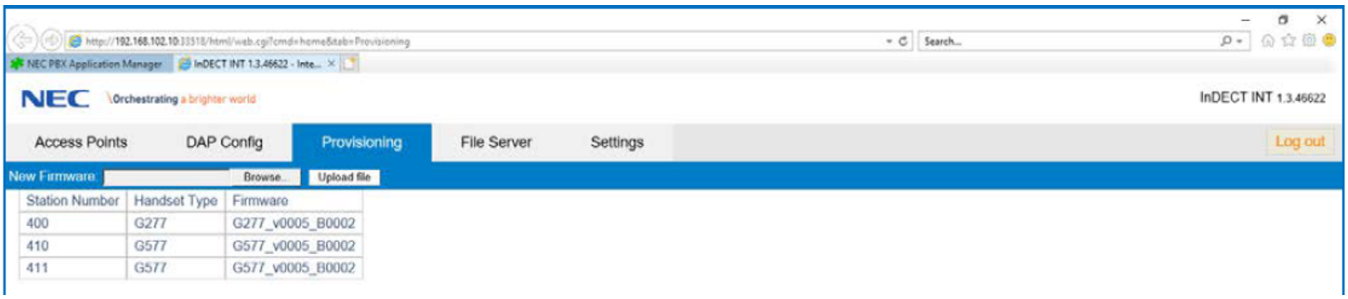
Items highlighted in orange are changes in the PBX configuration detected as different from the settings currently in the InDECT configuration file. Changes can be updated to the InDECT configuration by pressing the **Activate** button. You can check for any changes by pressing **F5** page at any time .

Items highlighted in blue are changes made to the InDECT DAP Config screen. Changes can be updated to the InDECT configuration by pressing the **Activate** button.

10.3 Provisioning Screen

Once your InDECT system is up and running, you can use the **Provisioning** screen to update the firmware on the handsets subscribed to the system. Further details on this feature can be found in the InDECT Additional Information Manual.

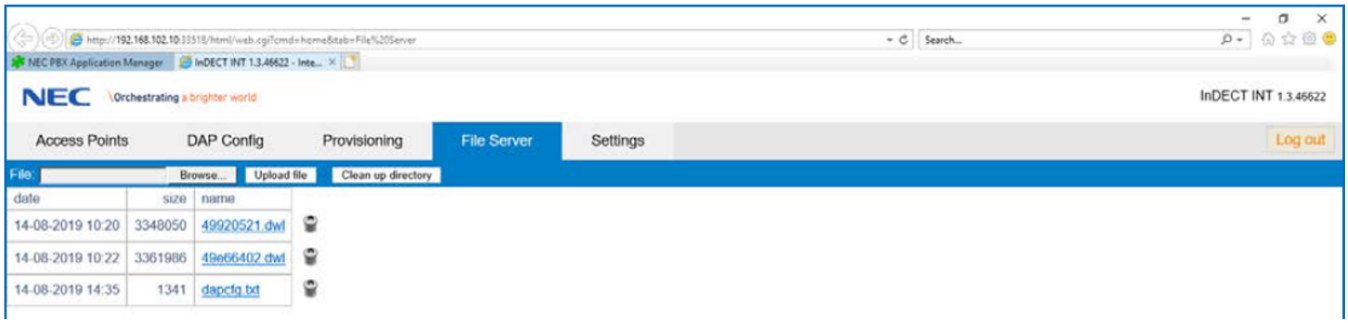
Figure 1-13 InDECT Provisioning Screen



10.4 File Server Screen

The **File Server** screen displays files stored on the PBX for the InDECT system to operate and the DAPs to download when connected to the system or rebooted for configuration changes.

Figure 1-14 InDECT File Server Screen



Files can be downloaded to the local device by clicking on the name of the file.

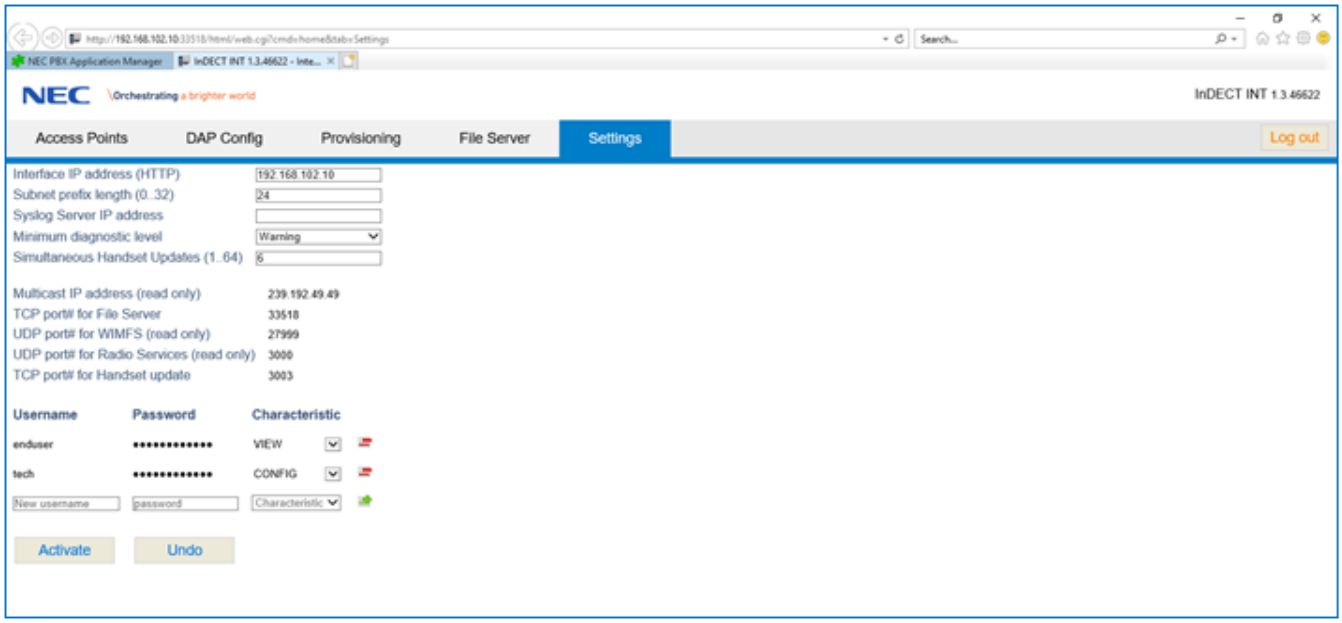
You can delete any files by pressing the **Delete** button next to the file name. If you delete the dapcfg,txt file this deletes the InDECT system configuration and you will be asked to create a new system.

10.5 Settings Screen

The **Settings** screen is used to check the InDECT HTTP provisioning IP address being used and also to allow for an external Syslog server to be configured for capturing SNMP logging information. You can also use the screen to create additional users with roles for accessing InDECT.

Further details on this feature can be found in the InDECT Additional Information Manual.

Figure 1-15 InDECT Settings Screen



SECTION 11 CREATING A NEW SYSTEM CONFIGURATION

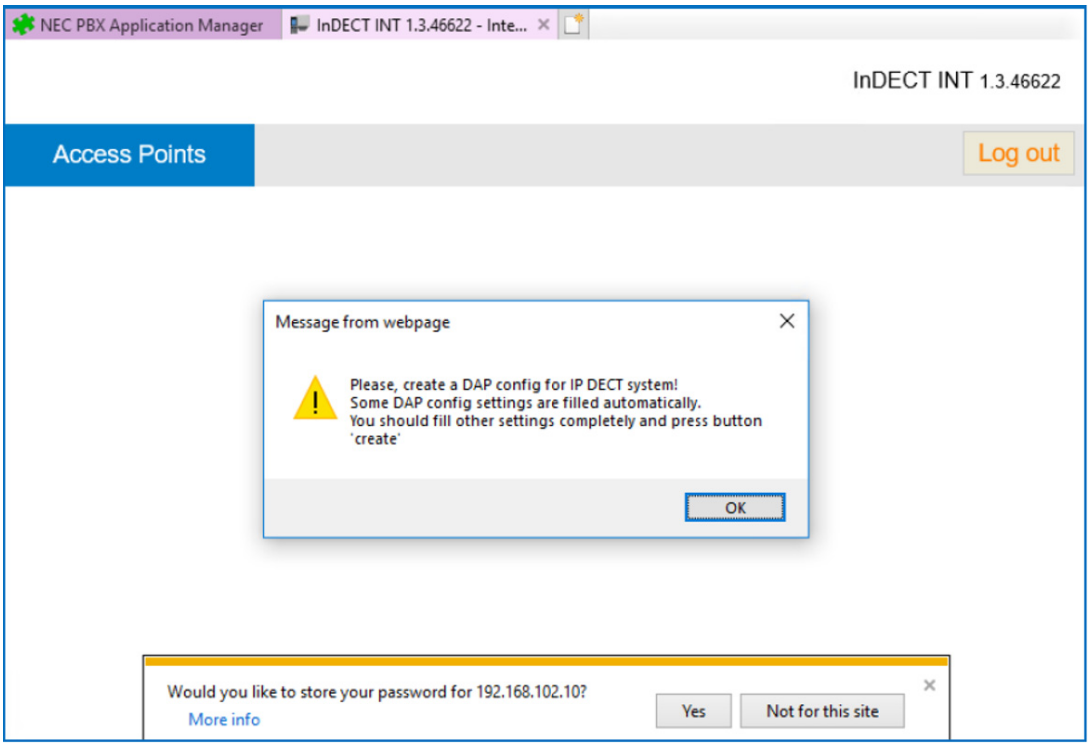
From the InDECT application manager screen, press the **Configure** 

button.

InDECT first checks to determine if a system configuration already exists on the PBX. If one is found, it opens the “DAP Config” window and displays the existing configuration.

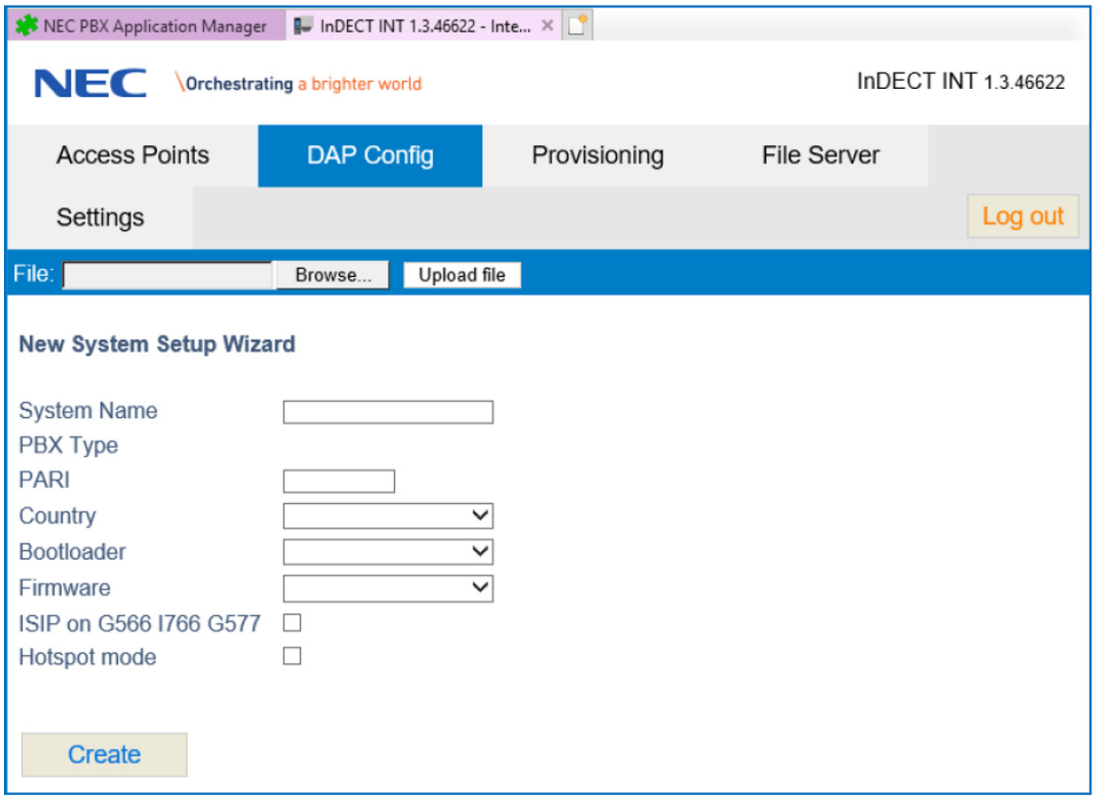
When you first run InDECT, or when it does not find an existing configuration file on the PBX, a notification displays to inform you that no system configuration has been found. Press the **OK** button to continue and create a new configuration.

Figure 1-16 InDECT Access Points – Notification



The **New System Setup Wizard** is displayed.

Figure 1-17 InDECT DAP Config – New System Setup



Fill in the following settings:

- **System Name** – This can be any given name for your InDECT system configuration.
- **PBX Type** – This will automatically be set by InDECT as either SV9100 or SL2100 depending on the PBX being used.
- **PARI** – The PARI (Primary Access Rights Identifier) code is a unique eight-digit identifier for InDECT. This provided to you when your InDECT order is processed.

  You must ensure you use an InDECT PARI from NEC. PARI codes purchased for other IP DECT solutions including IP DECT Lite/Unlicensed DAP Controller/Full DAP Controller systems cannot be used in conjunction with InDECT.
- **Country** – This determines the tone plan of the system and changes the DECT frequencies required for certain countries. This must be configured correctly for your installation location. If the country code is programmed in Program 10-02-01 of the PBX, InDECT can read this information and select the country automatically.

NOTE

It is recommended that you set the Country Code in the PBX first, as InDECT must be configured to the same country as the PBX.

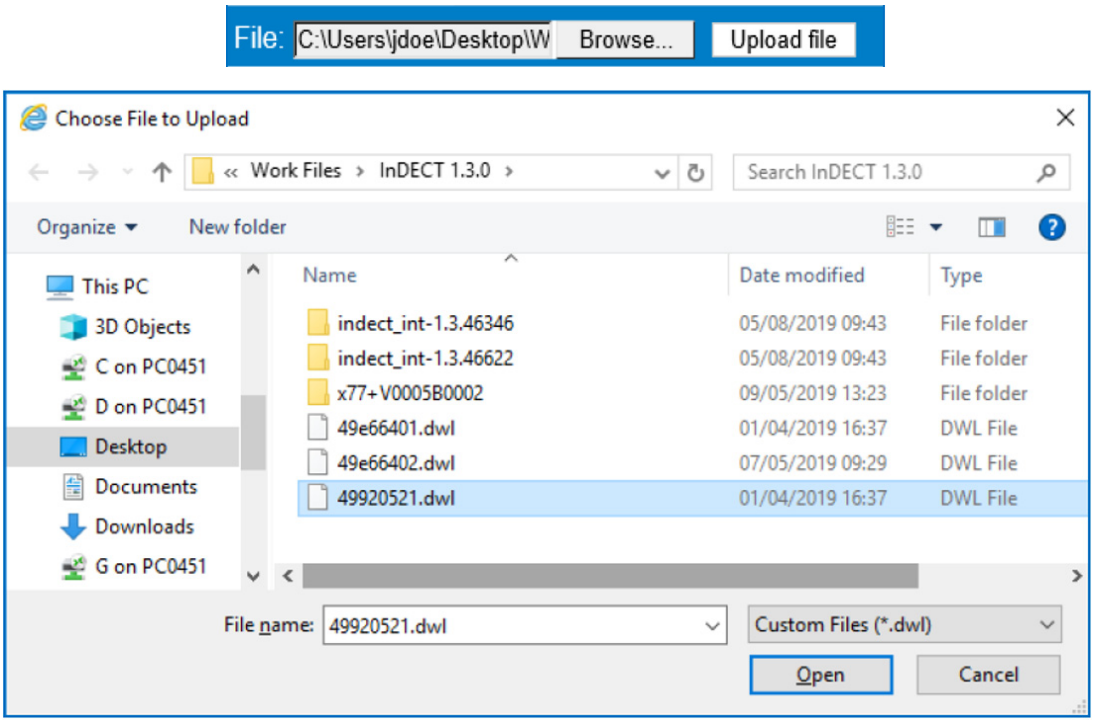
The supported countries for InDECT are: Algeria, Argentina, Australia, Austria, Bahrain, Belgium, Belorussia, Bolivia, Brazil, Bulgaria, Chad, Chile, China, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Gabon, Germany, Greece, Guatemala, Haiti, Honduras, Hong Kong, Hungary, Iceland, India, Indonesia, Iran, Ireland, Israel, Italy, Japan, Kenya, Korea, Kuwait, Latvia, Libya, Lithuania, Luxembourg, Macedonia, Malaysia, Maldives, Malta, Mexico, Montenegro, Morocco, Myanmar, Nepal, Netherlands, New Zealand, Nigeria, Norway, Oman, Pakistan, Panama, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sudan, Sweden, Switzerland, Syria, Taiwan, Thailand, Tunisia, Turkey, UAE, Ukraine, United Kingdom, Uzbekistan, Venezuela, Vietnam, Yemen.

- **Bootloader** – This is the loader package for the AP400 access point that controls its boot and start-up processes. Multiple files can be uploaded to the PBX, but this option selects the file to be used. It must be a minimum of **49920517.dwl** or newer for use with InDECT and the on-board file server.

  Before you can select a boot loader file, you must first upload one to the PBX. Follow the steps below to do this:

  1. Use the **Browse** button to locate a valid AP400 bootloader file. Press the **Open** button to select the file.

Figure 1-18 InDECT AP400 Bootloader File



2. Press the **Upload file** button to transfer to the InDECT file server. Wait for the progress bar to fill and the filename to appear in the Bootloader drop down list before continuing.

Figure 1-19 InDECT AP400 Bootloader File – Progress Bar

3. Once the required file uploads, you can select it using the drop down list control.

Figure 1-20 InDECT AP400 Bootloader File – Uploaded

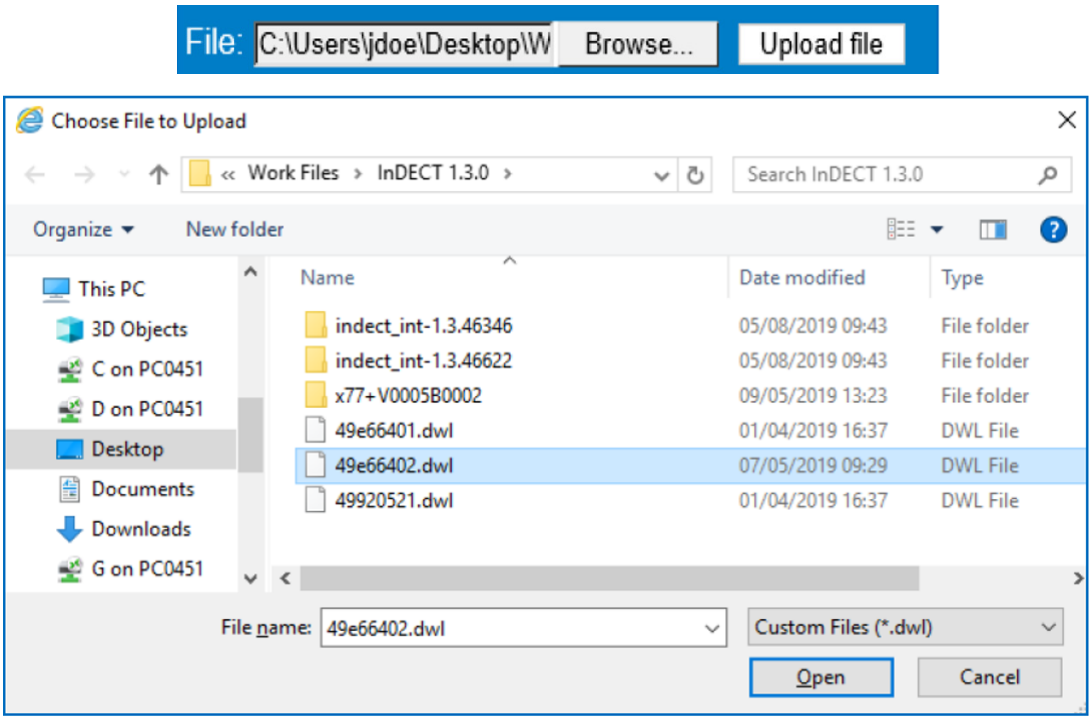
- **Firmware** – This is the firmware package for the AP400 access point that controls its operation while running. Multiple files can be uploaded to the PBX, but this option selects the file to be active. It must be a minimum of **49e66403.dwl** or newer for use with InDECT.

NOTE *All InDECT firmware packages use the format 49exxxxx.dwl.*

Before you can select a firmware file, you must first upload one to the PBX. Follow the steps below to do this:

1. Use the **Browse** button to locate a valid AP400 firmware file. Press the **Open** button to select the file.

Figure 1-21 InDECT AP400 Firmware File



2. Press the **Upload file** button to transfer to the InDECT file server. Wait for the progress bar to fill and the filename to appear in the Firmware drop down list before continuing.

Figure 1-22 InDECT AP400 Firmware File – Progress Bar

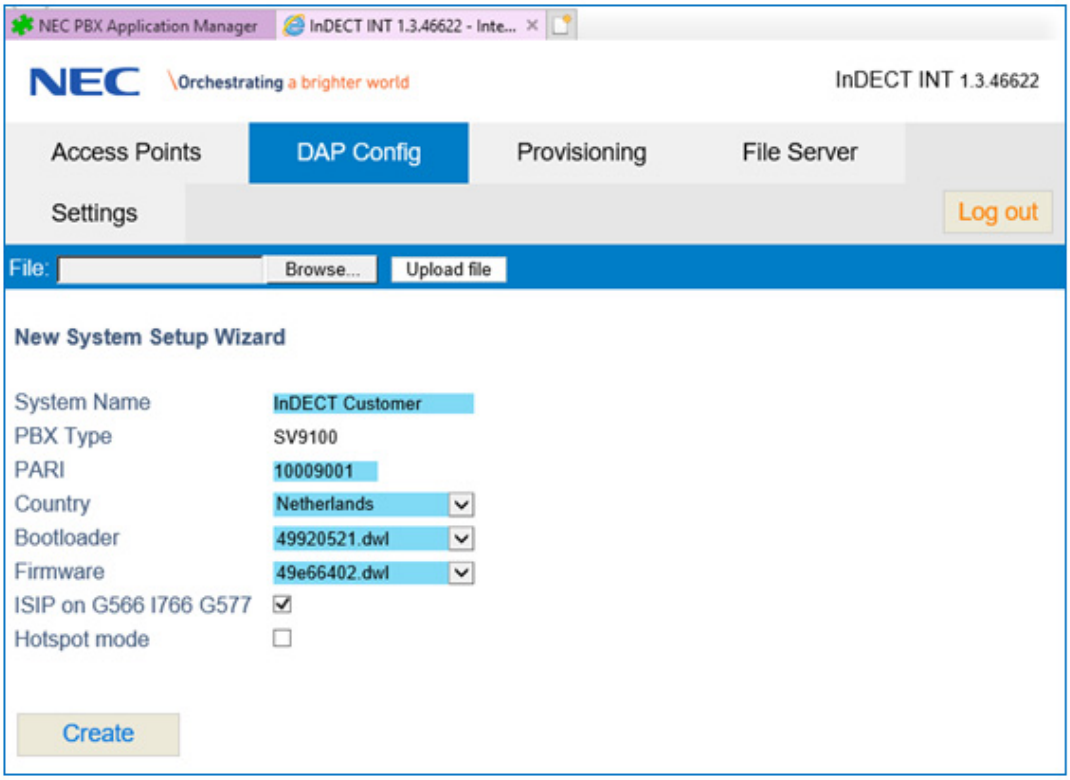
3. Once the required file is uploaded, it can be selected using the drop down list control.

Figure 1-23 InDECT AP400 Firmware File – Uploaded

❑ **iSIP on G566/I766/G577(h)** – This checkbox is optional and can be enabled to use the NEC iSIP protocol on either the G566/I766/G577(h) handsets. If this item is not checked, Standard SIP protocol is used.

- **Hot Spot Mode** – This checkbox is optional and can be enabled so that the individual DAPs do not synchronize over the air. Each individual DAP is a stand-alone “hot spot”.

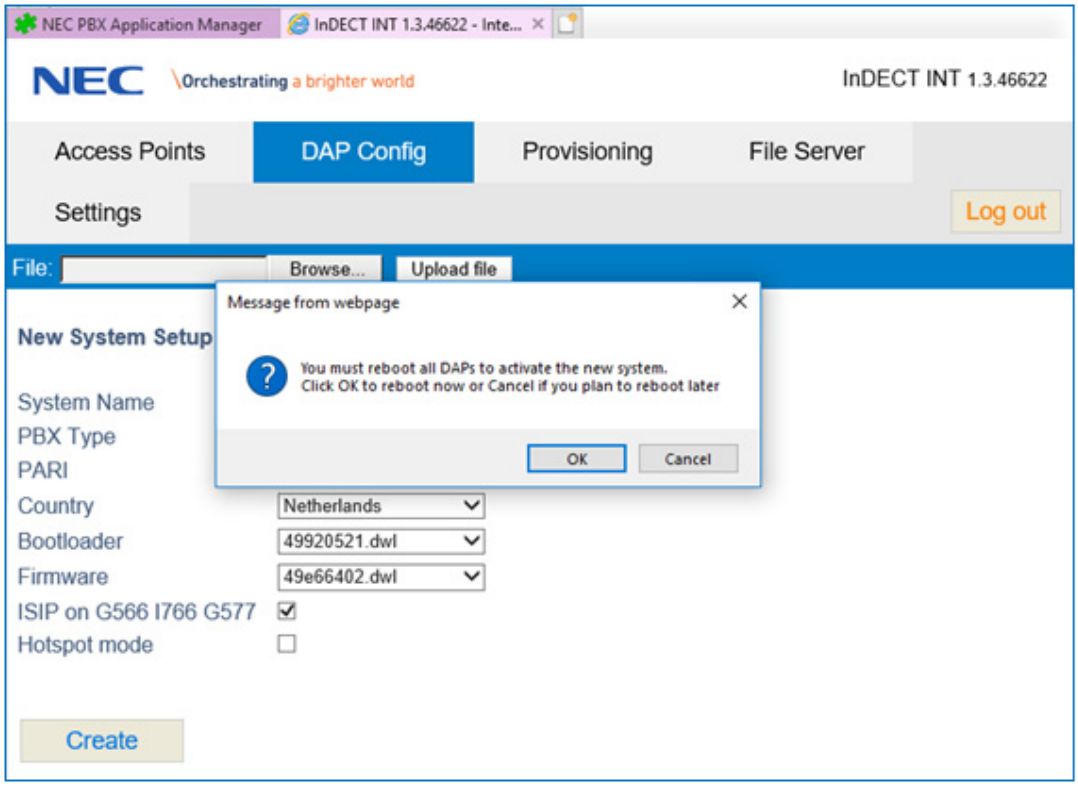
Figure 1-24 InDECT DAP Config – Hot Spot Mode



Press the **Create** button when ready. This creates your system configuration and generates the new InDECT dapcfg.txt file on the PBX file server.

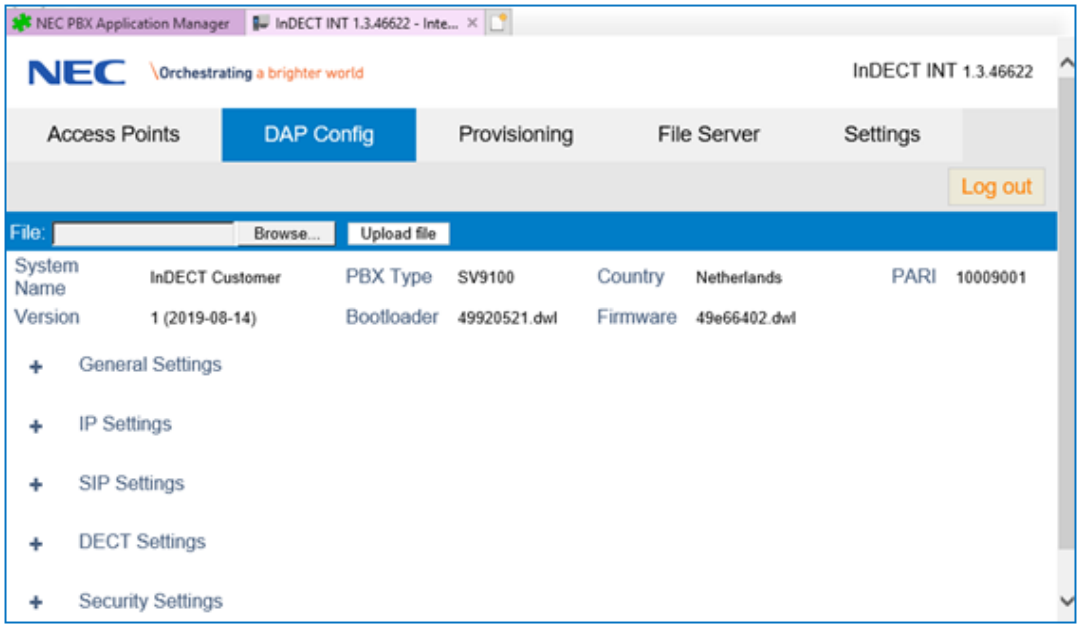
Once the **Create** button is pressed and the configuration file/firmware/bootloader packages are placed on the file server, InDECT automatically asks to reboot any connected access points so that they download the new configuration with any changes that have been made. If you wish to reboot any access points connected to the network at this time, press the **OK** button or press the **Cancel** button to ignore this and continue using InDECT.

Figure 1-25 InDECT DAP Config – Reboot Message



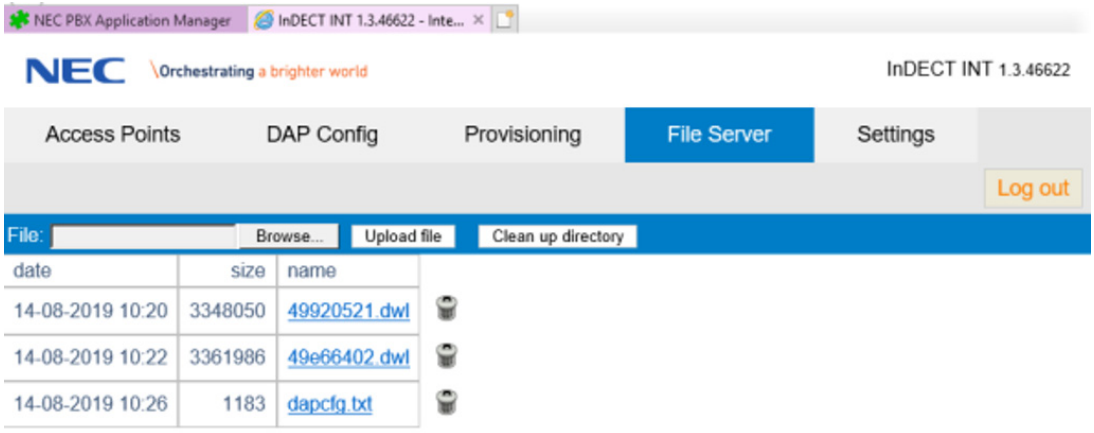
The first time a configuration is created, the version number in the dapcfg.txt file is set to 1. After this, any changes are made to your configuration file through the InDECT application, the version number increments to differentiate itself from the configuration file on your access points.

Figure 1-26 InDECT DAP Config Created



You can move to the **File Server** screen and should see listed the firmware package for the access point, the optional bootloader if required, along with the dapcfg.txt (configuration file).

Figure 1-27 InDECT File Server – Installed Files



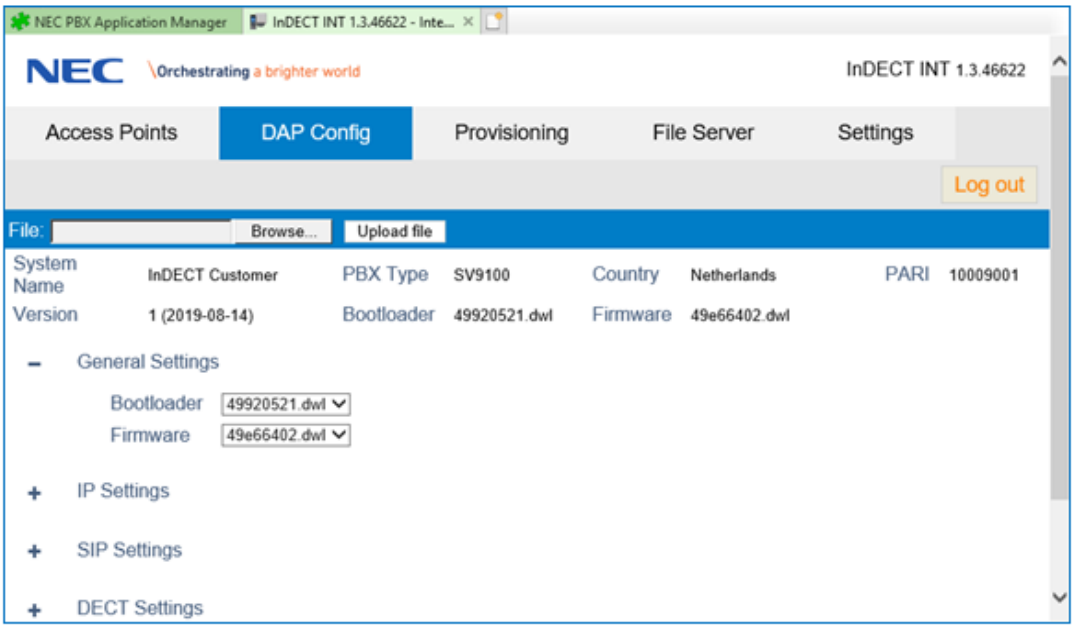
The basic system configuration is now complete. It is possible to review additional InDECT settings, if you wish, or modify your settings using the **New System Setup Wizard** screen.

InDECT automatically learns many of these items from the existing PBX configuration, but manual adjustments can be made to some of the items on the **DAP Config** screen. Automatically configured items must be adjusted through the PBX programming. If any changes are made to the PBX while you are still logged into InDECT, press the F5 key to refresh the screens and highlight any changed items.

The **DAP Config** screen is split into the following areas:

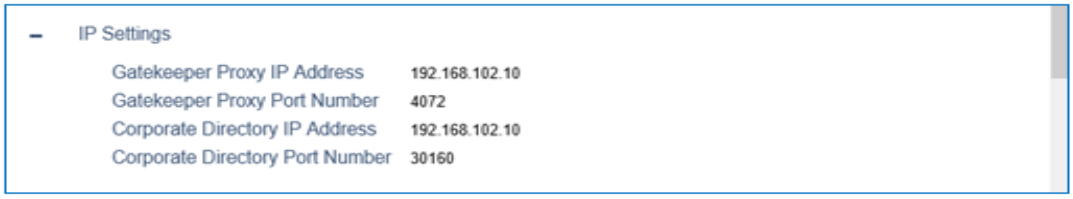
- **General Settings** – Here you can change the active firmware and bootloader files used. Switch between any uploaded files stored on the PBX fileserver.

Figure 1-28 InDECT DAP Config – General Settings



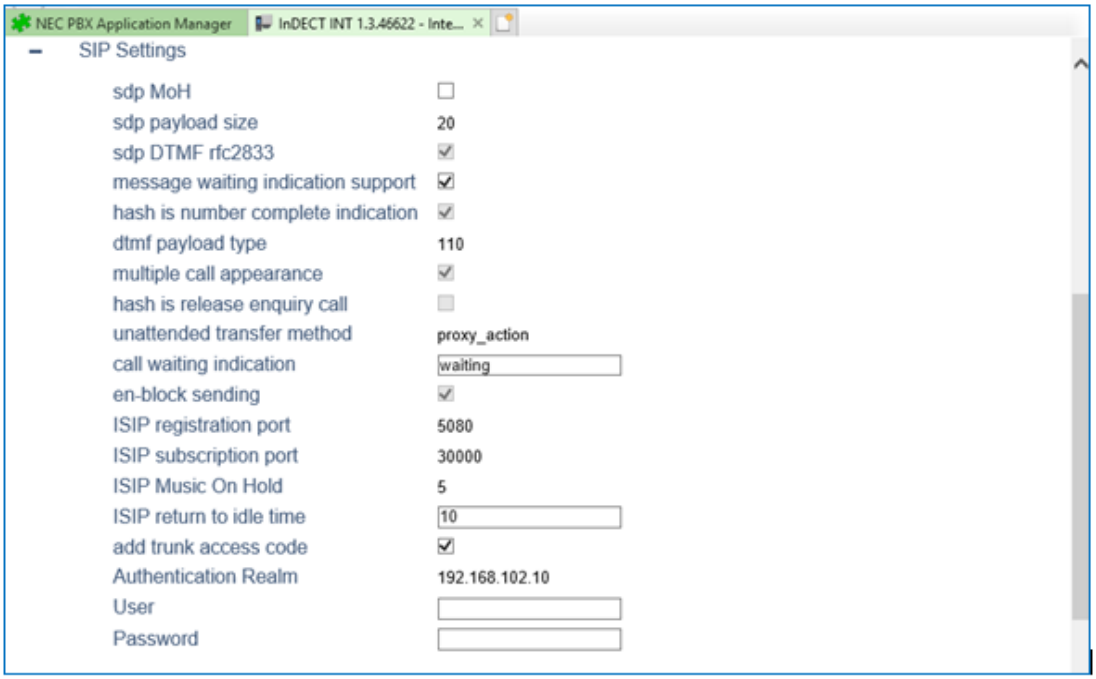
- **IP Settings** – This area shows the IP settings automatically set from the PBX configuration. These automatically configured settings are outlined in Appendix A, Section 1 IP Settings, which also refers to the PRG commands used to set them.

Figure 1-29 InDECT DAP Config – IP Settings



- **SIP Settings** – This area shows commonly configured SIP Settings used by InDECT. Settings automatically learned from the PBX are outlined in Appendix A, Section 2 SIP Settings, which refers to the PRG commands used to set them.

Figure 1-30 InDECT DAP Config – SIP Settings



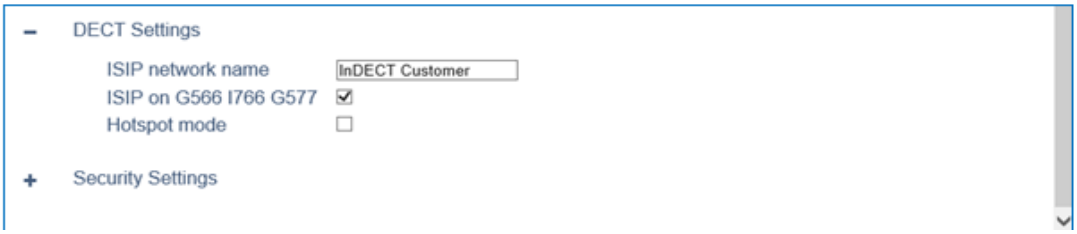
  - **sdp MoH** – When enabled, no local tone is generated by the access point when the IP DECT handset is on “hold” audio is provided by the PBX (recvonly mode). This can be edited.
  - **sdp Payload Size** – Offered payload size in the SDP (Session Description Protocol) offer (in ms). This item is automatically set from the PBX configuration.

- **sdp DTMF RFC2833** – When enabled, DTMF digits are sent according to RFC2833 (in RTP). Otherwise, the DTMF digits are sent as SIP “INFO” messages. This item is automatically set from the PBX configuration.
- **MWI Support** – Message waiting indication supported. This is supported by both SV9100 and SL2100 PBXs so can be enabled if required. Can be edited.
- **Hash Is Number Complete Indication** – The hash button can be used to indicate a number is complete or can be used as part of the dialed number. This is enabled by default.
- **DTMF Payload Type** – This parameter allows you to specify the DTMF payload type for RFC2833 implementation. The default value is 110 with the range between 96 ...127. This item is automatically set from the PBX configuration.
- **multiple_call_appearance** – When the handset is busy and a second call comes in, you hear a ticker tone and the display shows “waiting”. Use the * button, to toggle between the two calls. It behaves in a similar way as having a call on hold. This item is automatically set from the PBX configuration.
- **Hash_is_release_enquiry_call** – When you are in an inquiry call and you end up connected to a device like a voice mail server, you cannot hang up the phone without losing your call. In this case, you can press the # key to end your inquiry call while keeping your original call. This is disabled by default.
- **Call_waiting_indication** – Here you can specify the call waiting indication text, which is displayed on the handset when there is a call waiting. This item can be edited.
- **En-bloc (dialing)** – This is enabled by default.
- **iSIP Registration Port** – This item is automatically set from the PBX configuration.
- **iSIP Subscription Port** – This item is automatically set from the PBX configuration.
- **iSIP MoH Tone** – Set to Enabled; the value as 5 by default.
- **iSIP Return to Idle Time** – Set to 10 (seconds) by default. This item can be edited.
- **Add Trunk Access Code** – Set to Enabled by default. Can be edited.
- **Authentication Realm** – This item is automatically set from the PBX configuration.
- **Username** – If SIP authentication is used on the PBX, this setting is normally configured with the value “%s”. This item can be edited.
- **Password** – Enter the authentication password this is used during the registration process of the standard SIP DECT handsets. This should match the password entered in the PBX configuration for extensions in Program 15-05-16. This item can be edited.

- **DECT Settings** – This area shows some DECT specific configuration items. You can edit the following items:
  - **iSIP network name** – This can be any given name for your InDECT system configuration. It is displayed on the idle display of any iSIP DECT handsets.

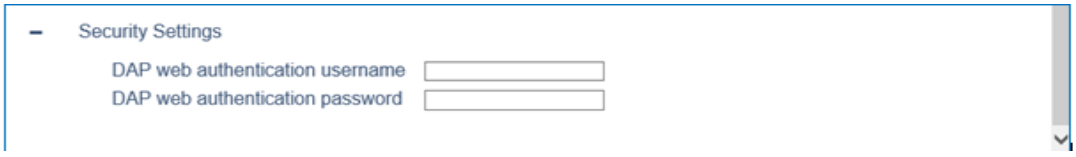
- **iSIP on G566/I766/G577(h)** – This checkbox is optional and can be enabled to use the NEC iSIP protocol on either the G566/I766/G577(h) handsets. If this item is not checked, the Standard SIP protocol is used.
- **Hot Spot Mode** – This checkbox is optional and can be enabled so that the individual DAPs do not synchronize over the air. Each individual DAP is a stand-alone “hot spot”.

Figure 1-31 DECT Settings – Hotspot Mode



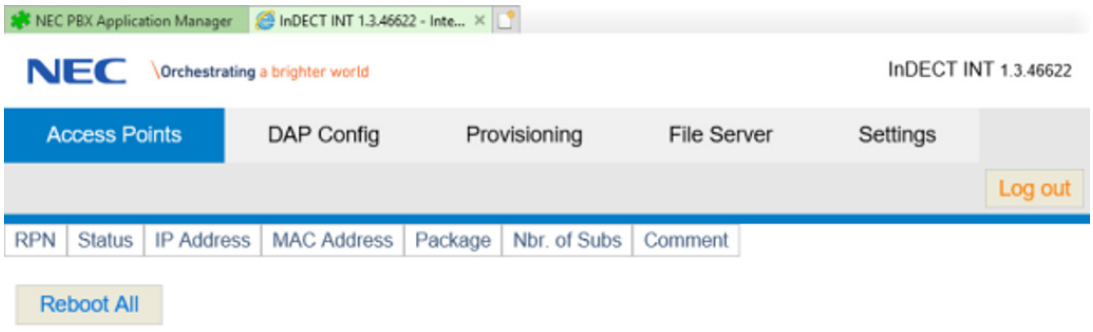
- **Security Settings** – This area provides some security configuration items for easily securing the DAPs WEB page used for handset subscriptions with a user name and password. You can edit the following items:
  - **DAP web authentication username** – Enter a username you want to use to access the DAP WEB page.
  - **DAP web authentication password** – Enter the password you want to use to access the DAP WEB page.

Figure 1-32 Security Settings – DAP Web Authentication



1. Go to the **Access Points** screen.

Figure 1-33 InDECT Access Points – Reboot All



2. Connect all access points to the InDECT PBX network. Wait until the system has detected all DAPs in the system and has transferred the loader, firmware and configuration files. This may take five minutes or more depending on the number of DAPs being connected.

3. After a while you should start to see access points being listed. They will automatically be allocated an RPN (Radio Part Number) and have their “Status” set as **New**. This means the access points are detected but not currently connected to the InDECT system. Wait until you see all access points that you require listed on the screen before continuing.

Figure 1-34 InDECT Access Points – Access Points Listed

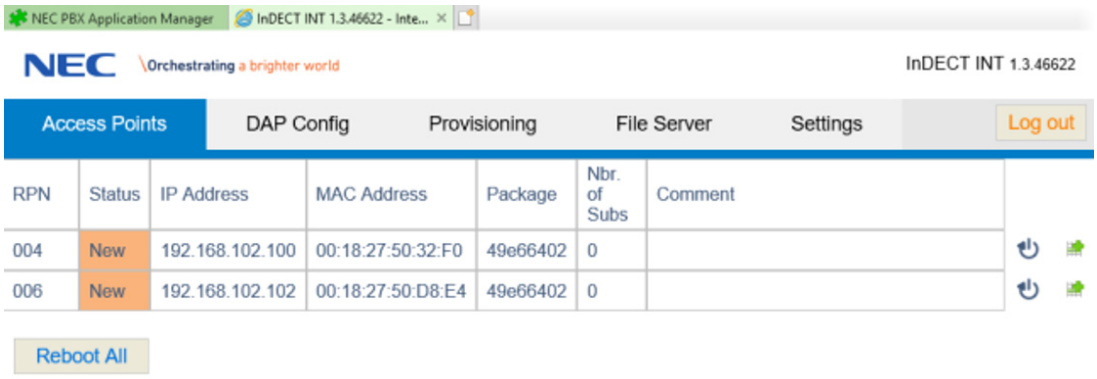
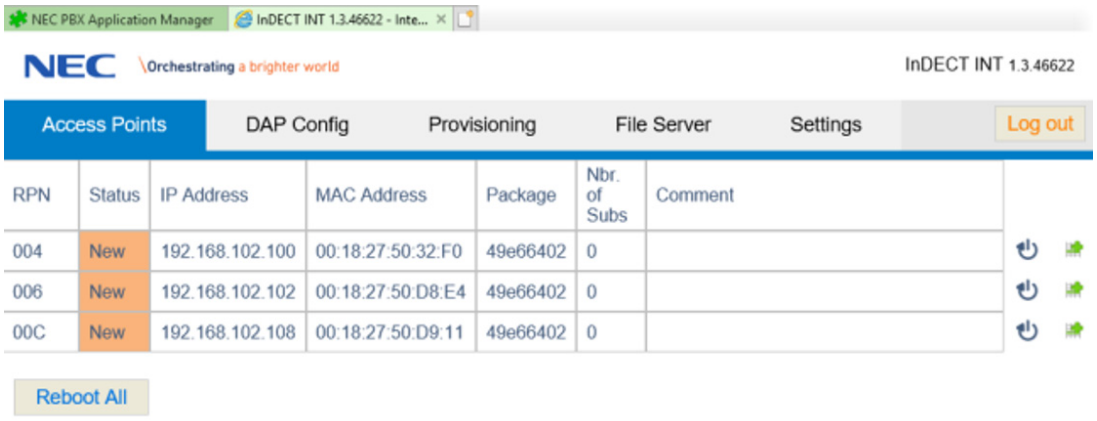
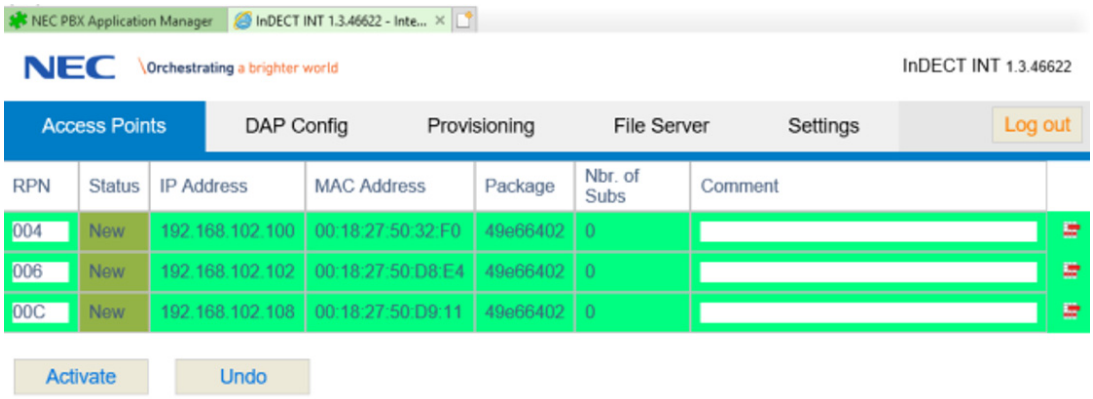


Figure 1-35 InDECT Access Points – All Access Points Listed



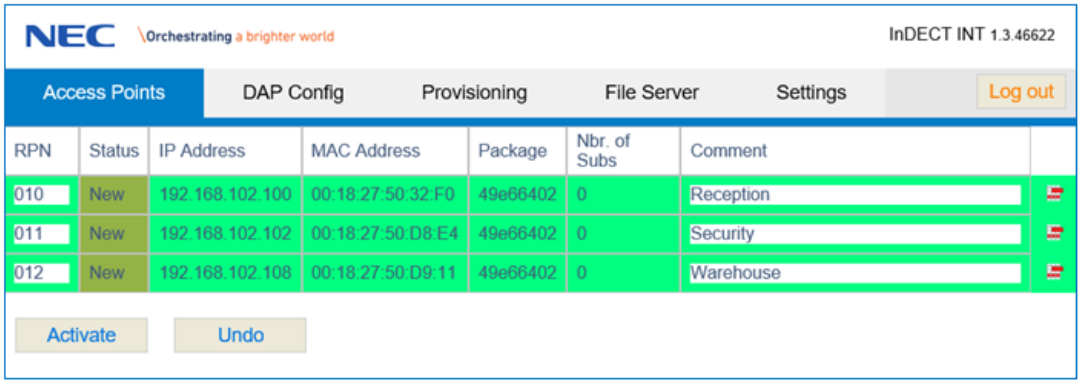
4. To add detected access points to your InDECT system press the **Add** button next to each access point. The selected access point row should change to green highlight.

Figure 1-36 InDECT Access Points – Add Access Points



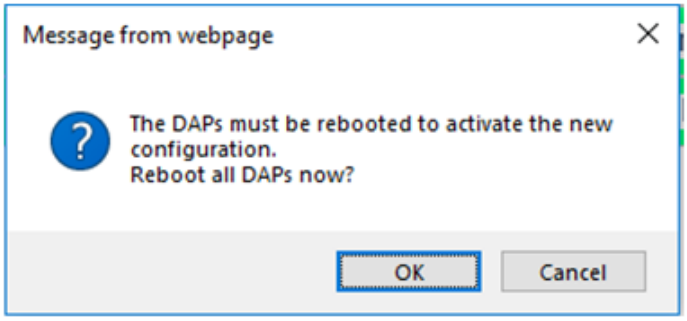
5. When you add an access point to your InDECT system, you can edit and reorder the RPN numbers assigned automatically by InDECT and you can also enter some descriptive detail in the comment field for each access point.

Figure 1-37 InDECT Access Points – Edit Access Points



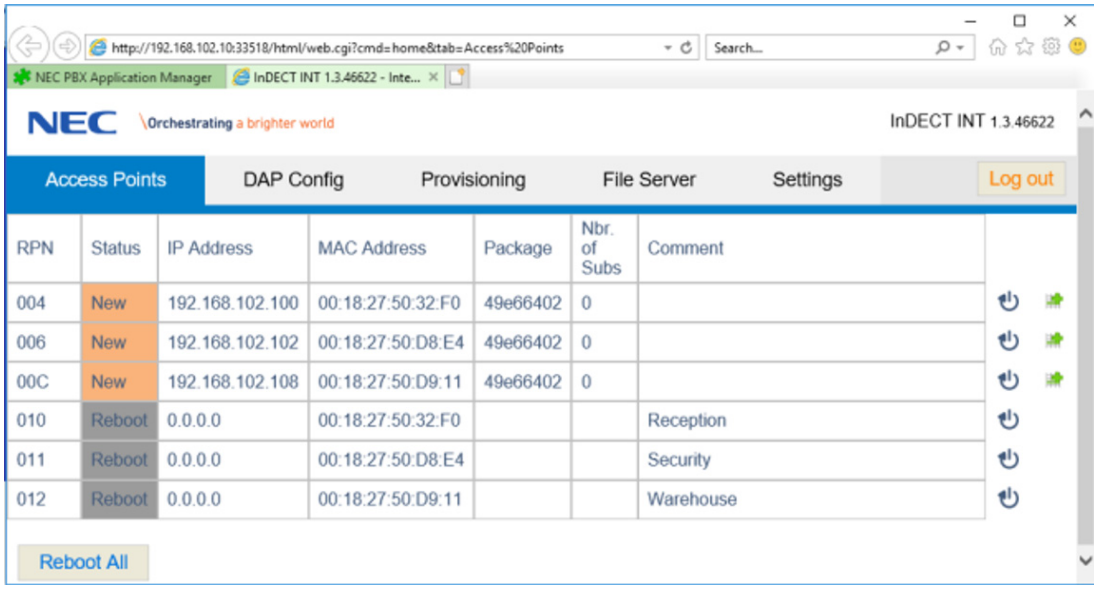
6. When ready to continue, press the **Activate** button. When the system asks for a reboot of all DAPs, press **OK** to reboot all DAPs.

Figure 1-38 Reboot All DAPs Message



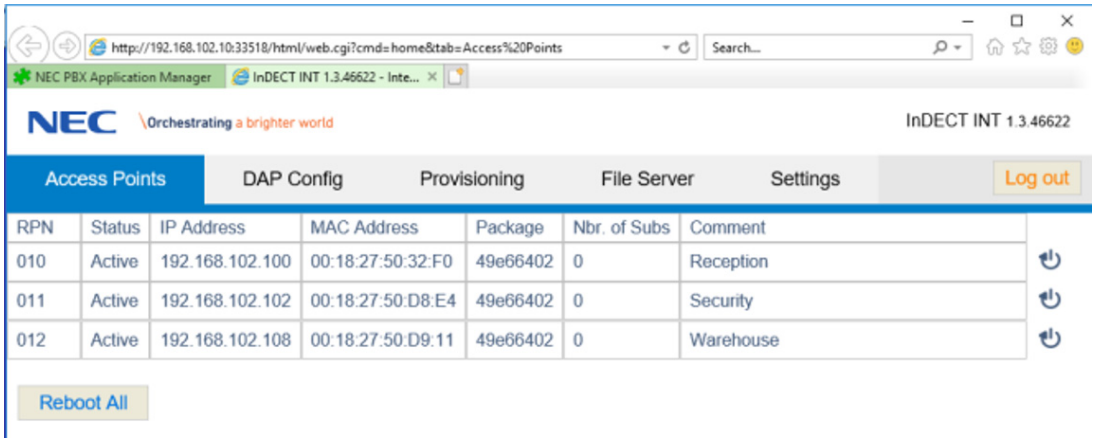
7. The DAPs reboot and are configured. After a few minutes if you have changed any RPN numbers, a screen similar to the one below displays.

Figure 1-39 InDECT Access Points – Example of Updated RPN Numbers



8. Once all DAPs are correctly provisioned and online, the system is ready to use after approximately 10 minutes.

Figure 1-40 InDECT Access Points – Provisioned and Online



9. To subscribe handsets, open the DAP WEB page for the DAP with the lowest RPN number from the Access Points screen. (In this case, click the IP address of the DAP with the lowest RPN number.).

SECTION 12 HANDSET SUBSCRIPTIONS

Before a handset can be used with the InDECT system, it must be made known to the system. This means that it must be "subscribed" to the system. The procedure is described in the following sections.

Please note, that each DAP holds a complete copy of **all subscription** records in the system. In case any of the DAPs are not working, you cannot subscribe handsets anymore. So make sure that all registered DAPs are up-and-running.

When a DAP that holds subscriptions is not working, the handsets will be unreachable for a time period of 5 minutes. After 5 minutes, the missing Subscriptions will be made active in other DAPs. This will make the handsets operational again.

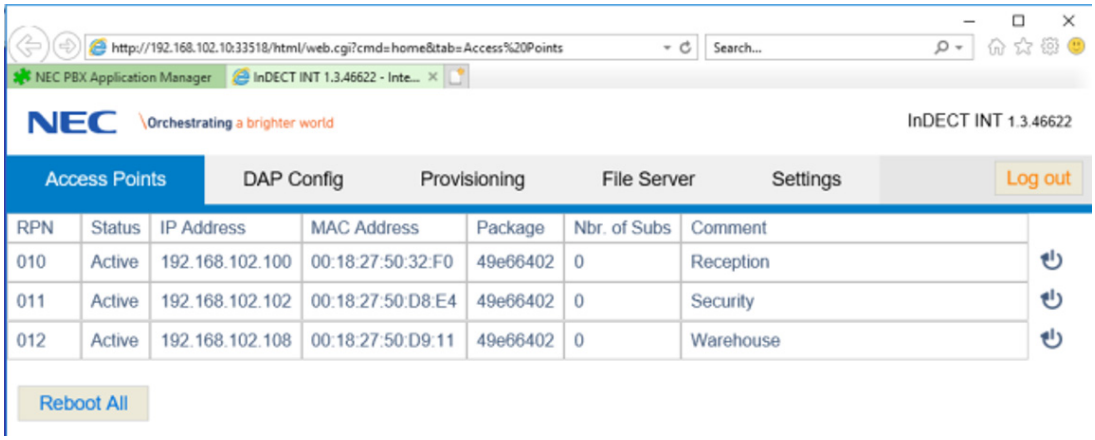
12.1 Subscribing a Handset

1. Open your WEB browser on one of the DAPs. Enter the following in the address bar:

   http://<DAP IP Address>/

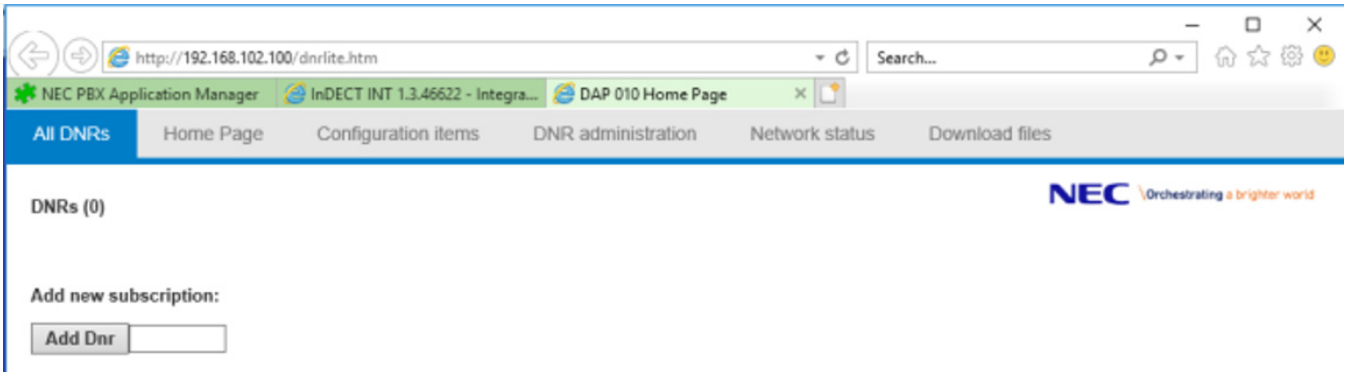
   or, click an IP address of a DAP on the Access Points screen.

Figure 1-41 InDECT Access Points – Example of Available IP Addresses



The following window is displayed:

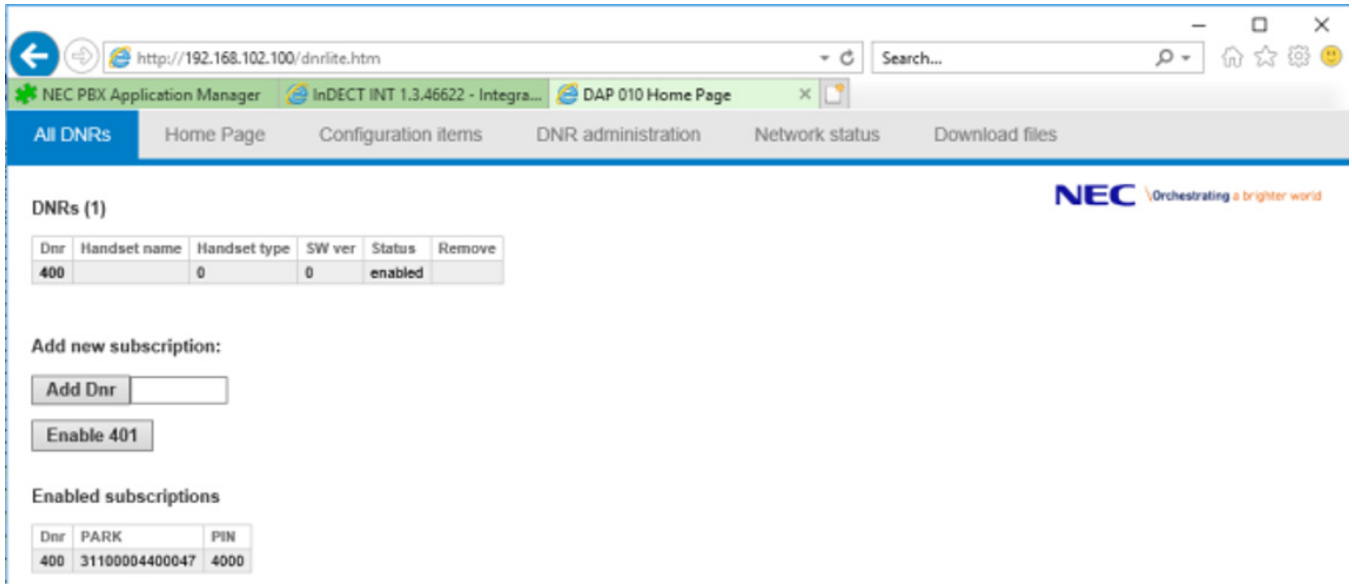
Figure 1-42 InDECT – All DNRs



NOTE *Verify that any "POP-UP Blocker" in your WEB Browser is switched OFF. If not, you will not see the Add Dnr button.*

2. Enter an extension number and press **Add Dnr**. The system is now ready for a subscription. A PARK and PIN code are displayed.

Figure 1-43 InDECT – Add DNRs



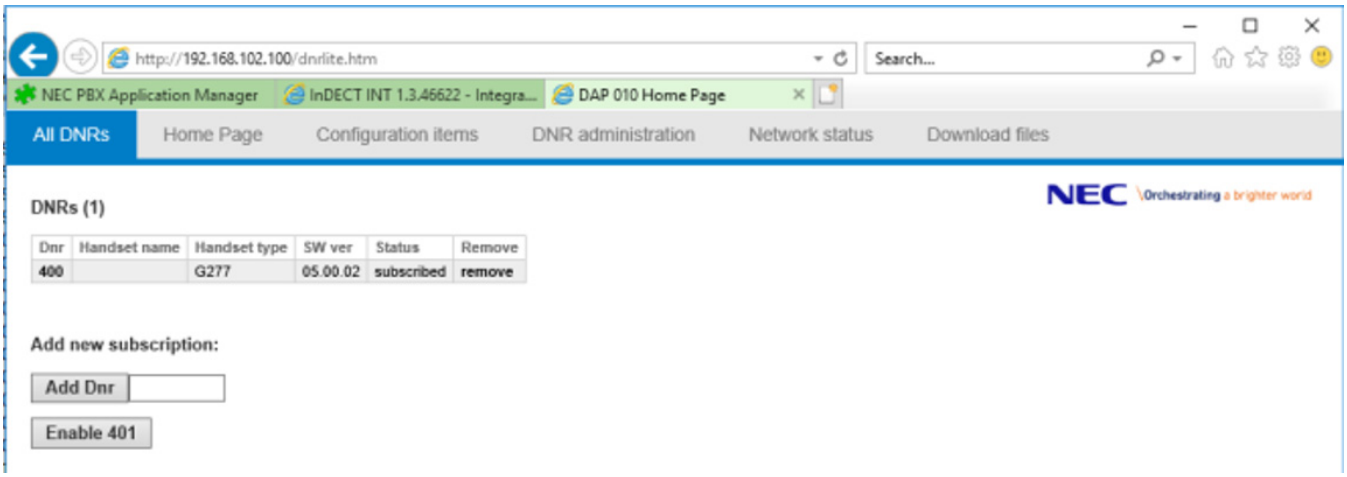
3. Execute the subscription procedure on the handset within three minutes. If necessary, consult the handset documentation to understand the subscription procedure for your particular handset. *The subscription procedure is active for three minutes only.* On the handset enter the PARK and the PIN code that is displayed for this DNR subscription.

NOTE

When the subscription is no longer active, or the subscription was successful, the WEB page is not immediately updated automatically. Click <F5> to refresh/update the WEB page.

After you have entered the extension numbers, he following window (with example extension numbers) displays. You can easily enable the next extension number by pressing the “Enable X” button. If you want to enter an extension number other than the proposed number on the button, enter that extension number in the field next to **Add Dnr**.

Figure 1-44 InDECT – Enable DNRs

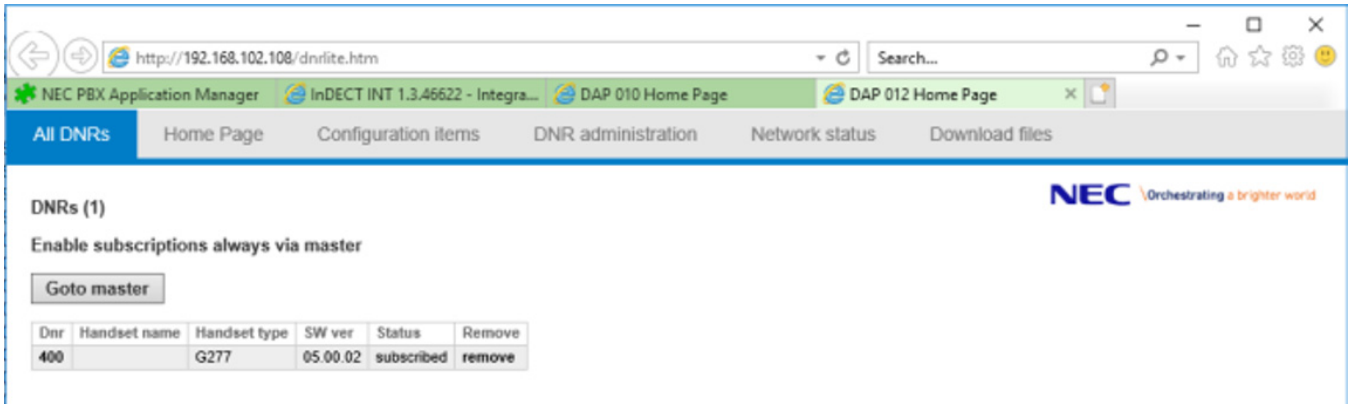


If you are in the WEB page of a DAP other than the DAP with the lowest RPN number, the following WEB page displays.

NOTE

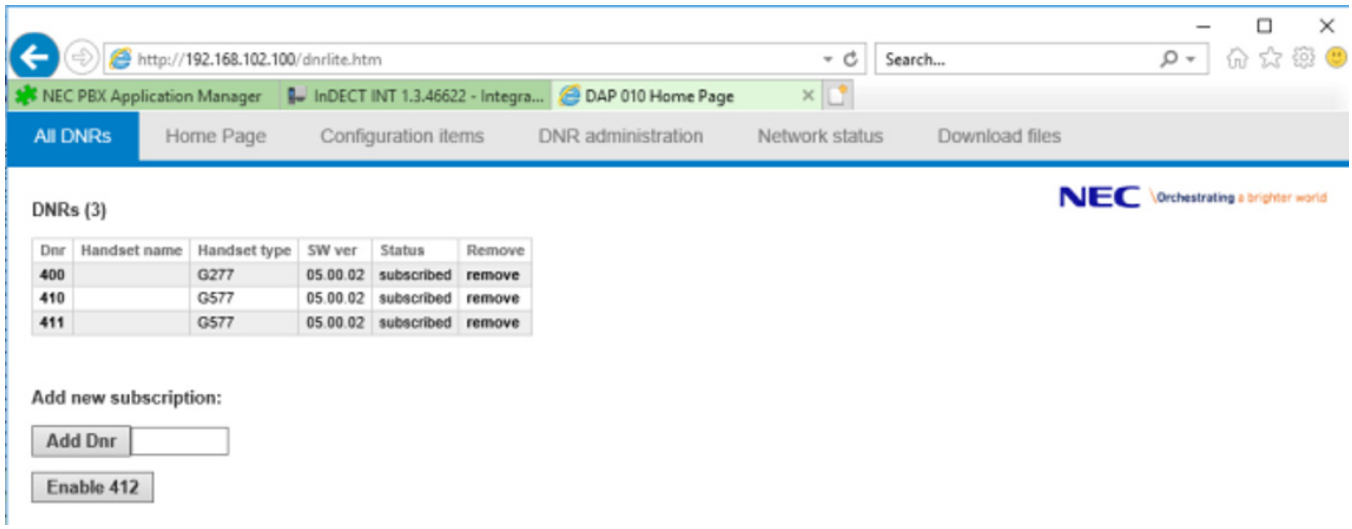
Verify the POP-UP blocker is switched OFF in your browser.

Figure 1-45 InDECT – Enable Subscription



You see that in the WEB Page other than the DAP with the lowest RPN number, you cannot subscribe handsets. However, you can remove handsets. When you want to subscribe a new handset, you have to go to the DAP with the lowest RPN number. From a WEB page on a DAP, which is not the master, you can easily go to the WEB page of the master, by pressing the button **Goto master**.

Figure 1-46 InDECT – Example of Subscribed Handsets



12.2 Removing a Handset

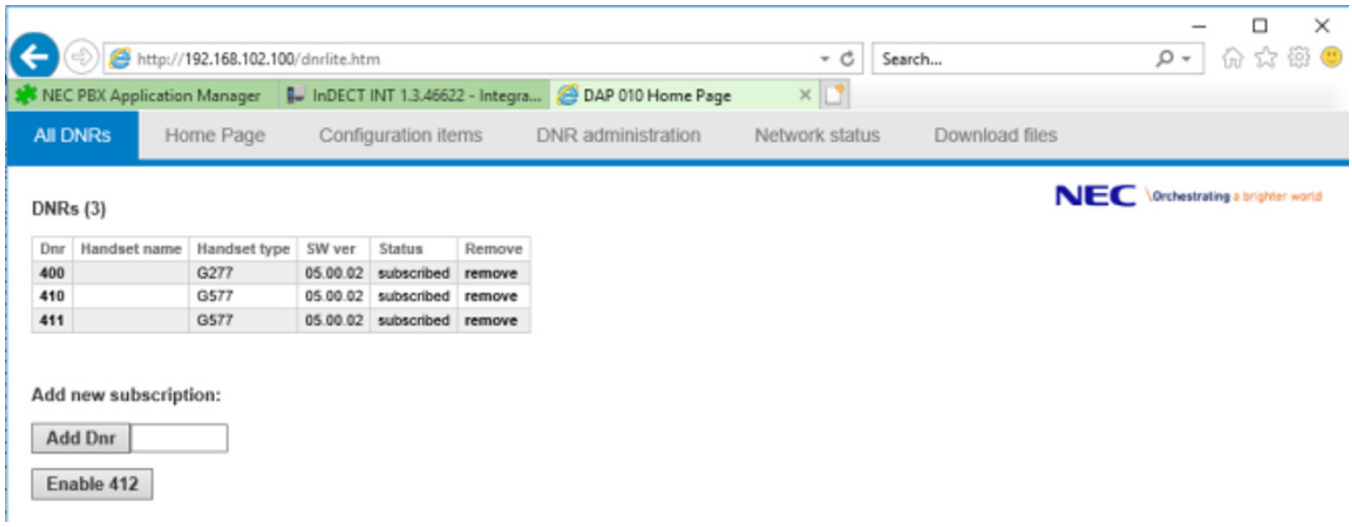
1. Open your WEB browser on one of the DAPs. Enter the following in the address bar.

   http://<DAP IP Address>/

   or, click an IP address of a DAP on the Access Points screen.

   The following window is displayed.

Figure 1-47 InDECT – Removing a Handset



Verify the handset, which you want to de-subscribe, is switched on and within DAP coverage. Press **Remove** behind the subscription row of the extension you want to remove.

In a few moments, the subscription is removed from the system as well as from the DECT handset.

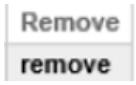
NOTE

The extension status in the WEB page is not automatically updated. To verify the remove action was successful, press <F5>.

When the extension number is not visible anymore (after a refresh), the remove action was successful. However, mark the following note:

NOTE

When the handset is not within DAP coverage, or broken or lost, the "Remove DNR" status changes to "Terminate".



If this occurs, click "Terminate." The subscription data is removed from the IP DECT DAP Lite system, but not from the handset! You must remove the subscription data manually from the handset (if possible).

2. When the remove action was successful, the extension number disappears from the list. (Press <F5> to refresh the status.).
3. To subscribe the same number again, follow the procedure in section 12.1 Subscribing a Handset on page 1-30.

SECTION 13 MAKING CHANGES IN THE CONFIGURATION

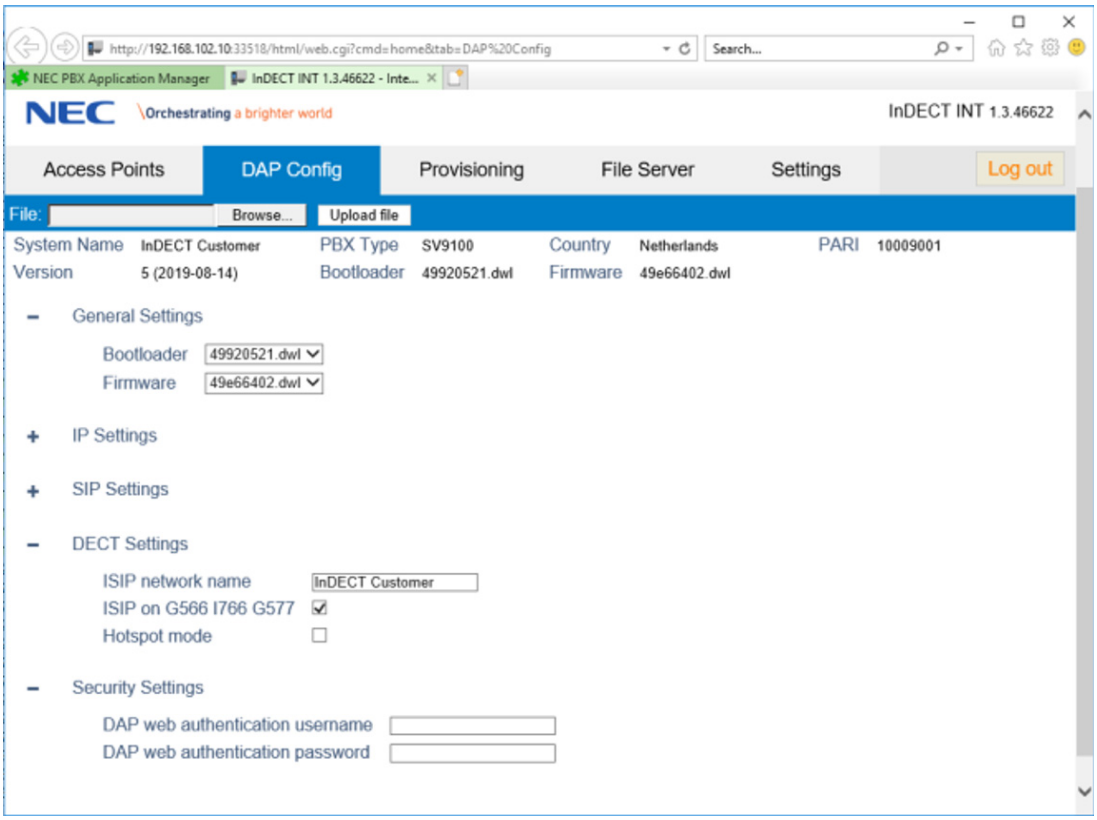
You can easily make changes to your InDECT configuration once the system is up and running.

From the InDECT application manager window, press the **Configure** 

button.

InDECT checks for a system configuration on the PBX. If it finds one, it opens the “DAP Config” window and displays the system settings.

Figure 1-48 InDECT DAP Config – Example of System Settings



Items highlighted in orange are changes in the PBX configuration that are detected as different from the settings currently in the InDECT configuration file. Changes can be updated to the InDECT configuration by pressing the **Activate** button. You can check for any changes when on this page at any time by pressing **F5**.

Items highlighted in blue are changes made to the InDECT DAP Config screen. Changes can be updated to the InDECT configuration by pressing the **Activate** button.

Make the required changes, then click the **Activate** button in the bottom left corner to apply them to your system configuration.

Press the **Undo** button to revert back to previous settings.

SECTION 14 UN-INSTALLING INDECT

Before un-installing InDECT, you should understand that when the application is un-installed any existing configuration and associated system files are removed. To keep a backup of the current configuration you should first download the system files from the **File Server** screen to a safe location.

1. To remove the application, go to the application manager and stop InDECT if it is already running.

   Press the **Stop** 

   button to stop the InDECT application service.

2. Once the application has stopped and you are ready to remove it, press the **Remove** button. This un-installs InDECT from the PBX. Confirm twice that you want to remove the application.

Figure 1-49 InDECT – Remove Application

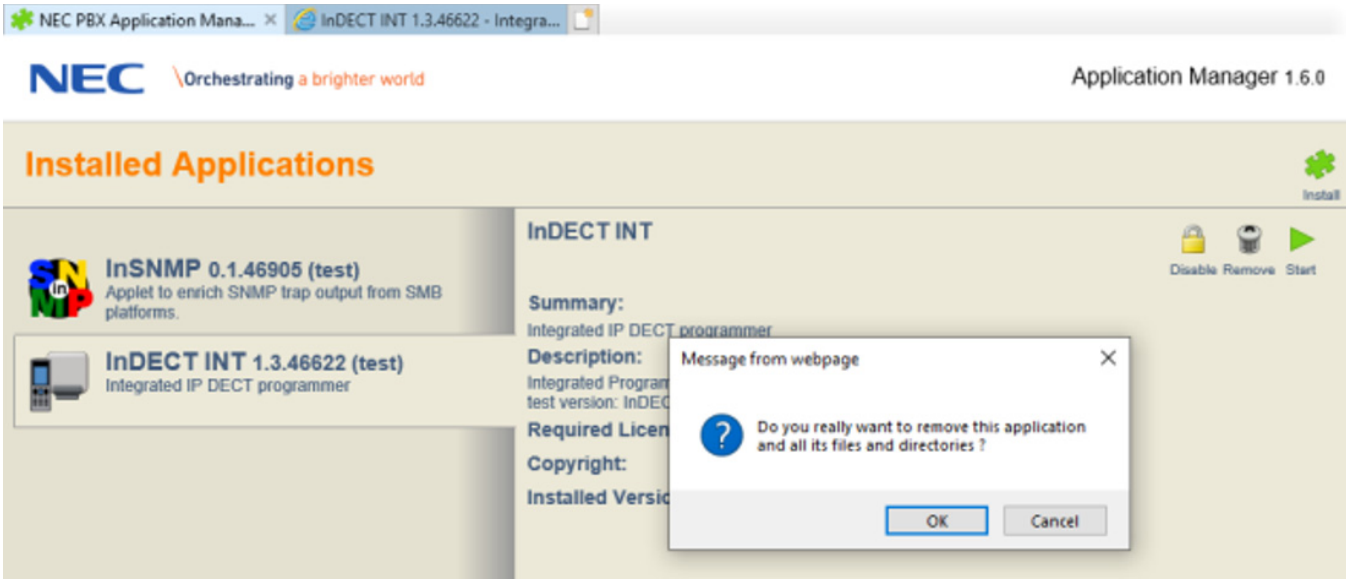
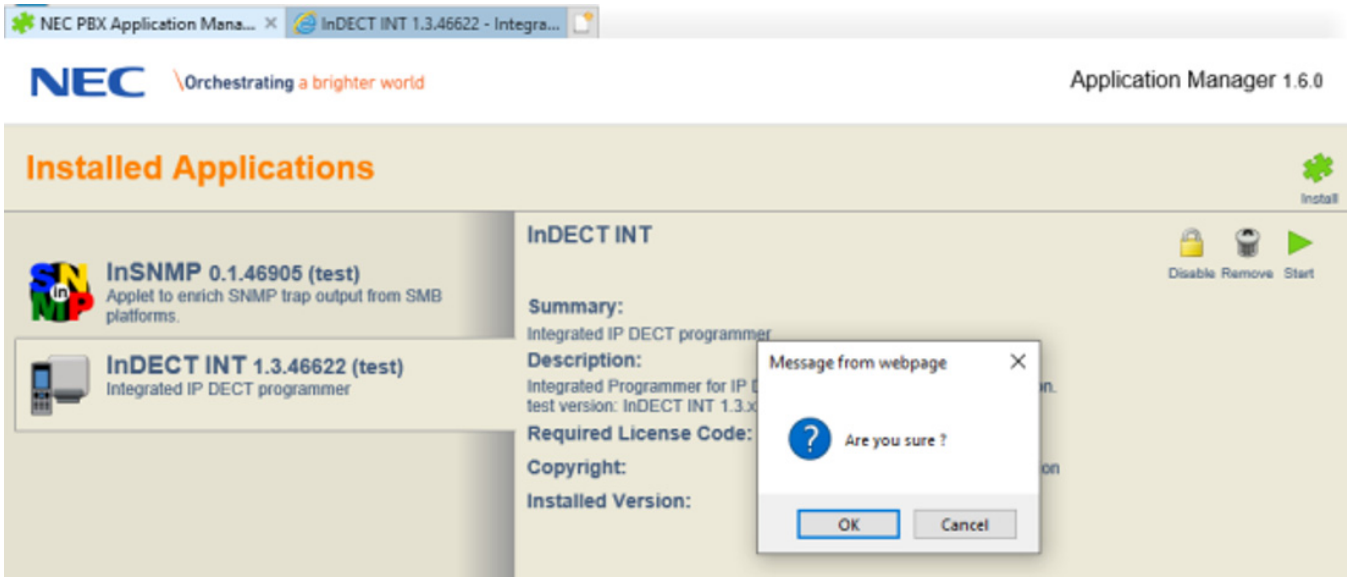


Figure 1-50 InDECT – Confirm Remove Application



SECTION 15 UPGRADING INDECT

Before upgrading InDECT, you should note the current version that is installed and make a backup of the current system configuration files by downloading them, using the “File Server” screen to a safe location.

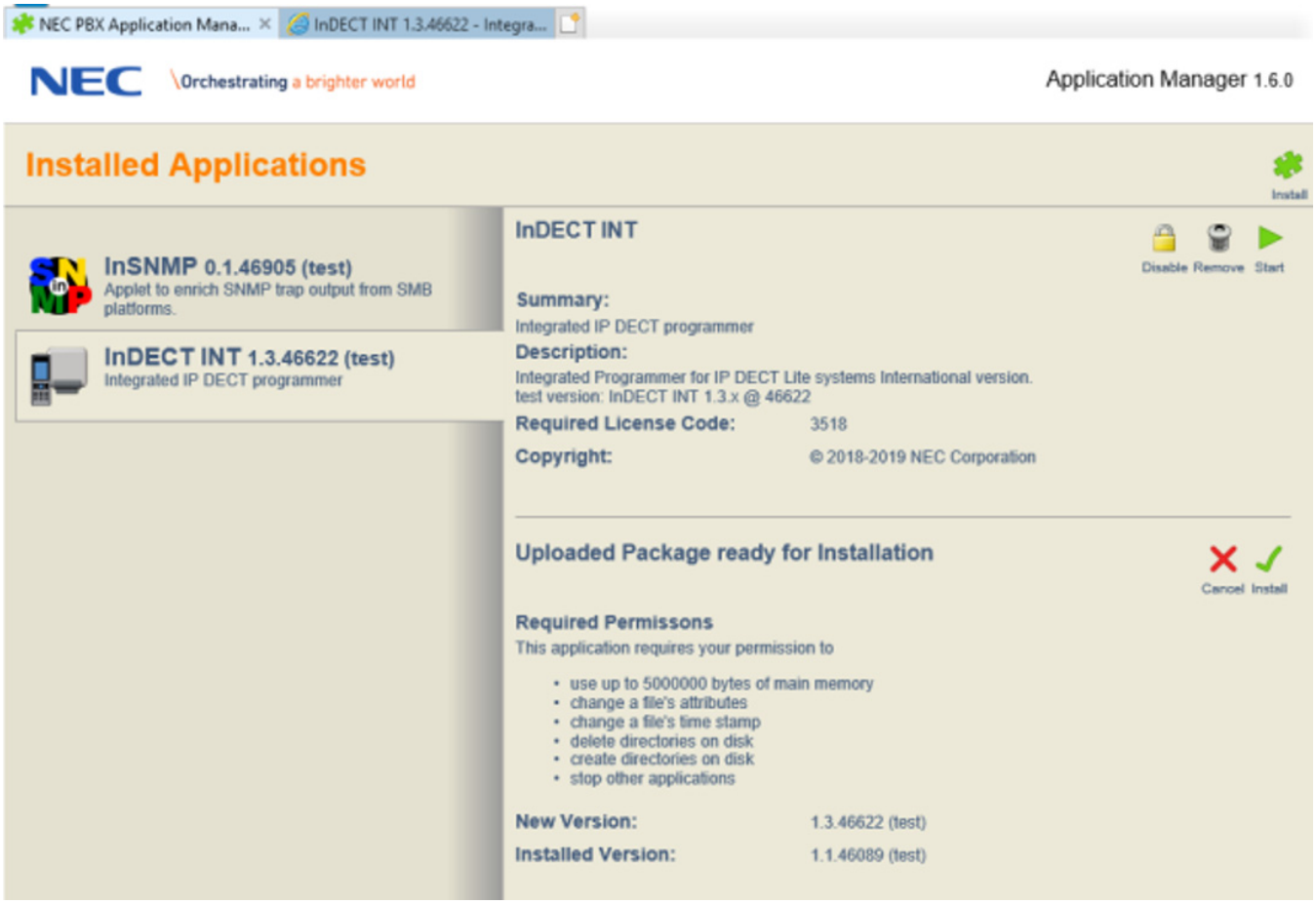
The existing configuration is automatically available after the upgrade competes.

After a backup has been performed, stop InDECT from the Application Manager.

Once it stops, install the new version. The application manager shows the currently installed version and the new version to be installed.

3. Click the **Install** button to proceed with the upgrade.

Figure 1-51 InDECT – Example of Upgrading InDECT



4. The upgrade may take up to one minute. Once complete, the application starts and you are able to access it again.

PBX Items Configured by InDECT

Appendix A

SECTION 1 IP SETTINGS

The following table lists IP settings for the SV9100 and SL2100 systems.

Table A-1 IP Settings

IP Setting	SV9100 Programming	SL2100 Programming
Gatekeeper Proxy IP Address	PRG10-12-09	PRG10-12-09
Gatekeeper Proxy Port Number	PRG84-20-01	PRG84-20-01
Corporate Directory IP Address	PRG10-12-09	PRG10-12-09
Corporate Directory Port Number	PRG10-20-14	PRG10-20-14

SECTION 2 SIP SETTINGS

The following table lists SIP settings for the SV9100 and SL2100 systems.

Table A-2 SIP Settings

SIP Setting	SV9100 Programming	SL2100 Programming
sdp Payload Size	PRG84-19-01	PRG84-19-01
sdp DTMF RFC2833	PRG84-34-01 Device Type 04 – SIP Extension	PRG84-34-01 Device Type 04 – SIP Extension
DTMF Payload type	PRG84-34-02 Device Type 04 – SIP Extension	PRG84-34-02 Device Type 04 – SIP Extension
Multiple call appearance	PRG20-13-53	PRG20-13-53
iSIP Registration port	PRG10-46-06	PRG10-46-06
iSIP Subscription port	PRG10-46-12	PRG10-46-12
Authentication realm	PRG10-12-09	PRG10-12-09